

THE BUG BOOK

Also in this series:

- #1 The Explosives Primer
- #3 Advanced Explosives Technology

VECTOR TECHNOLOGY VOLUME 2
THE BUG BOOK
copyright ©1989 VECTOR PRESS

ISBN 1 875110 04 6

Published by VECTOR PRESS, P.O. Box
434, Brighton S.A. 5048.

This book is copyright. With the exception of any use classified as fair dealing under the Copyright Act, it may not be reproduced in whole or in part by any process without the written permission of the publisher.

Neither the author nor the publisher assume any responsibility for the use or misuse of the information contained herein. This book is sold for informational purposes only.

INTRODUCTION

This, the second volume in the Vector Technology series deals with electronic surveillance in all its manifestations: wireless microphones, telephone tapping, laser eavesdropping, and debugging.

In dealing with these topics our aims have been two-fold; to present to the reader a comprehensive, qualitative discussion of eavesdropping technology, and to provide circuit diagrams so that the more electronically-inclined may experiment.

In line with the first aim, we have adopted much of the text of the U.S. Government Commission Reports on Wiretapping and Electronic Surveillance, which provide a complete and well-researched framework. In line with the second, this has been updated, corrected and supplemented. We hope you will enjoy this book.

If you have any comments, questions or additional information, please feel free to write (c/o Vector Press).

Please Note: Neither the author nor the publisher intends that the material in this book should be used for any purpose which is unlawful. This book is for information purposes only.

CONTENTS

AUDIO EAVESDROPPING 4

Telephone Systems 4....Telephone Wiretapping 6/ Wire Systems 6/ Radio Systems 9/ Accessories 12...Telephone Eavesdropping 15/ Infinity Transmitters 15/ Listen-backs and Keep Alives 17/ On-line Microphones 17/ Telephone Modifications 18/ Radio Frequency Flooding 19/
Microphone Systems 19....Types of Microphones 21/ Carbon 21/ Magnetic 21/ Speakers 22/ Condenser 22/ Electret 24...Special Purpose Microphones 24/ Contact, Spike and Pneumatic 24/ Shotgun and Parabolic 26/
Radio Eavesdropping 28....Inexpensive Devices 28/ Wireless Microphone Transmitters 29/ Fabrications 29...Drop Transmitters 29/ Miniature Devices 29/ Modulation Techniques 32...Carrier Current Devices 33...Microwave Devices 34...Passive Reflectors 36...Remote Switch Receiver 36 Tape Recording Systems 36 Optical Directional Systems 36...Other Devices 41

AUDIO SECURITY COUNTERMEASURES 44

Telephone Systems 44....Telephone Taps 44/ Wire Systems 44/ Radio Systems 46...Telephone Room Eavesdropping Devices 47/ Infinity Transmitters 47/ On Line Microphones 48/ Telephone Modification 48
Radio Eavesdropping Device Detection 49...Field Strength Measurement 50...Countermeasures Receivers 52...Spectrum Analysis 55...Other Inspection Equipment 57 General Purpose Audio Surveillance Protection Systems 57...Acoustic Protection 57...Radio Frequency Protection Systems 59.

GLOSSARY 60

Audio Eavesdropping

Audio eavesdropping, or "bugging" is accomplished primarily through the use of various electronic devices and technical processes. A complete audio eavesdropping system requires a device that will convert audible sounds into electrical signals and communicate these signals via radio transmitter, wire, or light beam to the eavesdropper. This book describes those devices which are capable of performing all or part of the eavesdropping process and the characteristics and limitations of each device. Further, wherever possible, circuit diagrams are included for experimental and explanatory purposes.

Initially, the discussion centres on the telephone system and its role in audio eavesdropping technology, but it progresses to include radio transmitters, microphones, tape recorders and optical devices that are used today in various forms of audio surveillance.

Telephone Systems

The standard telephone functions as a small part of a vast electronic system which is operated by the telephone company. The company provides all of the power to operate the subscriber telephones, the automatic switching equipment which connects one instrument to another, and the various electronic signals which cause dial tones, ringing and busy signals. Some of these features may be used by the eavesdropper to advantage in telephone surveillance. He may use the voltage present on the wires to supply power to electronic devices, the wires themselves to carry audio signals that have been converted to electrical signals, and the handset as an eavesdropping microphone.

Telephone audio eavesdropping can be accomplished by two methods that involve connecting various electronic devices to this system. The first and most widely publicised method uses wiretap paraphernalia which intercepts conversations directly from the telephone wires and requires no entry into the target premises. The second method is that which uses a portion of the telephone system for room eavesdropping and usually requires physical entry into the premises. This method is possible because the telephone instrument with its associated wires and electronic parts can be made to monitor room conversations with minor electrical modifications. A diagram of a standard telephone instrument is shown in figure 1. This schematic illustrates portions of the telephone which are susceptible to modification or additions and likewise illustrates the technical complexity of some forms of electronic eavesdropping. Below the diagram is a list of telephone system oriented eavesdropping devices which are included in the discussion presented in this and the following paragraphs.

The standard telephone instrument consists basically of (1) a

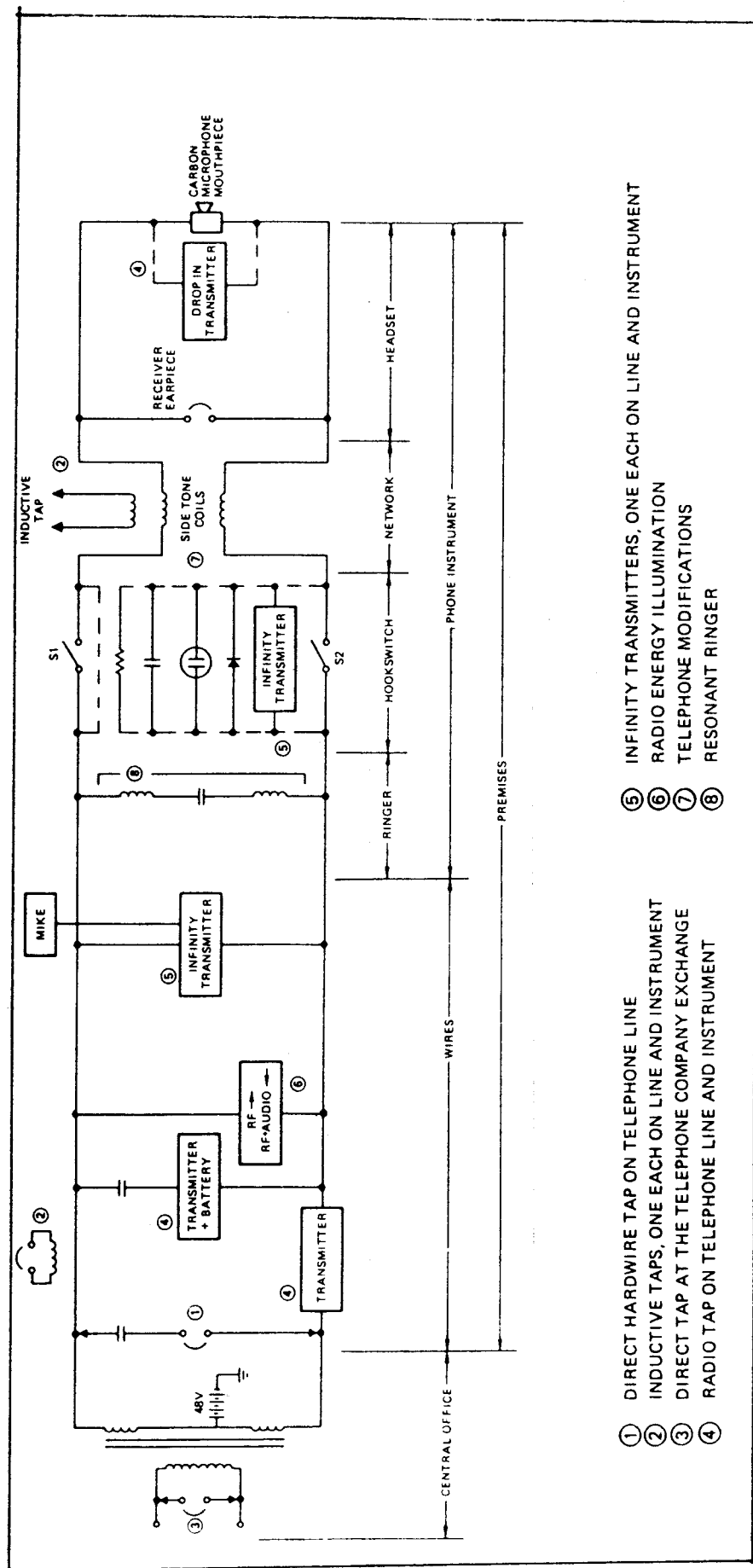
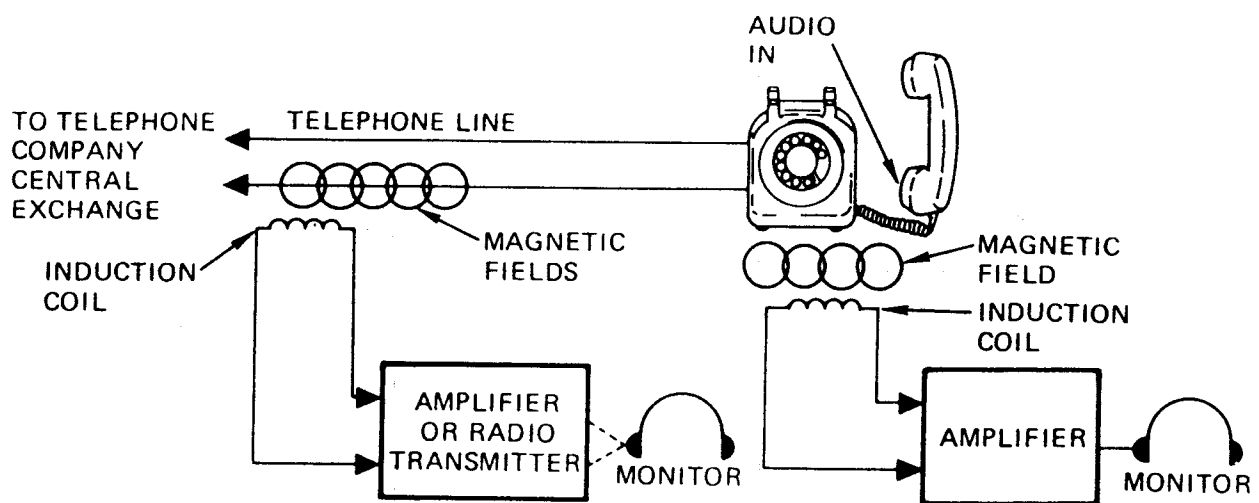


FIGURE 1: TELEPHONE SYSTEM EAVESDROPPING

microphone, or mouthpiece, which converts the speaker's voice into the electrical signals that are sent through the telephone's internal circuitry and out onto the wires; (2) an earpiece, a magnetic device which receives electrical signals from another telephone and converts these signals back into audible sound; and (3) a dial mechanism which generates the electrical pulses used by the telephone company central switching exchange to identify the dialled telephone number. A switch, which ordinarily keeps these components separated from the external lines when the telephone is not being used, is activated by a spring loaded button or lever when the handset is lifted from its cradle. The switch, shown as S1 and S2 in figure 1, is called a hook-switch. It plays an important role in the practice of audio eavesdropping. The terms, "off hook", meaning that the telephone is in use, and "on hook", meaning that the instrument is not being used are commonly used expressions in any discussion regarding the telephone instrument and will be frequently used here to describe the operating status of the instrument. When the telephone handset is lifted off-hook, the line voltage drops from 48 volts to between 6 and 12 volts, and 60 to 100 milliamperes of current flow through the instrument. This current is modulated by sound waves striking the carbon mouthpiece and passed through the telephone's internal circuitry to the outgoing wires or "talk pair". These signals continue through the telephone company's electronic switching system to the receiving telephone. Here, incoming electrical signals are converted back into audible sounds by the magnetic earpiece. By manipulating these features and exploiting their intended purpose, the eavesdropper is assisted in the process of audio surveillance.

Telephone wiretapping. The term telephone wiretapping describes a procedure or activity which requires the use of several electronic and mechanical pieces of equipment. The process consists of identifying the specific telephone talk pair of interest at some accessible location along the wires, the interception of their electrical signals, and the communication of these signals to the eavesdropper's tape recorder or headphones. The electronic devices which can accomplish the interception and communications portion of this process are numerous and, with the exception of miniature tap transmitters, are readily available.

Wire Systems. The initial step in the wiretapping procedure involves the connection of electronic equipment to the telephone wires to retrieve the audio electrical signals. Proper equipment and installation procedures must be used to assure a good quality wiretap and to prevent easy detection by the telephone company or security inspection team. Two methods are used by professionals which are equally difficult to detect. The first uses a wire coil to inductively couple the audio signals from the lines while the second, more conventional method uses a direct wire connection and electronic matching equipment. These techniques are illustrated in figures 2 and 3.



MAGNETIC FIELD SURROUNDING TELEPHONE WIRE AND INSTRUMENT IS PROPORTIONAL TO THE AUDIO SIGNAL

INDUCTION COIL TRANSFORMS MAGNETIC FIELD VARIATIONS TO AN ELECTRICAL SIGNAL

LOW LEVEL ELECTRICAL SIGNALS ARE AMPLIFIED FOR AUDIO MONITORING OR RADIO TRANSMISSION

Figure 2: Inductive Sensing

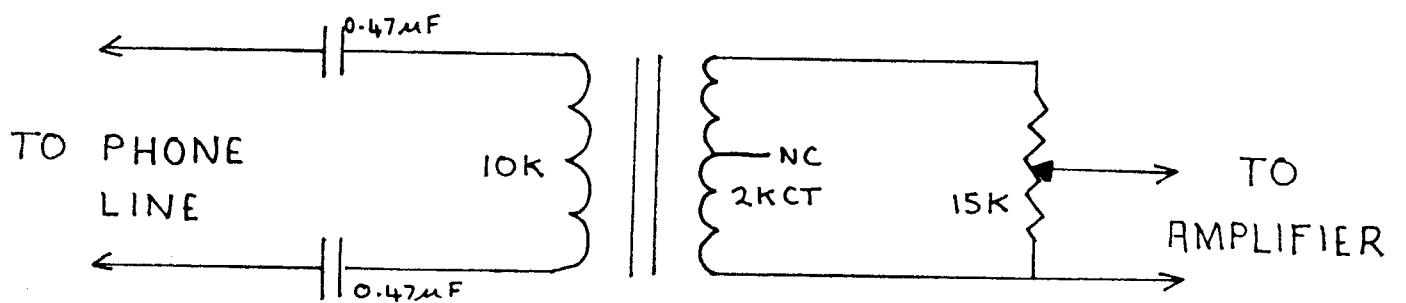
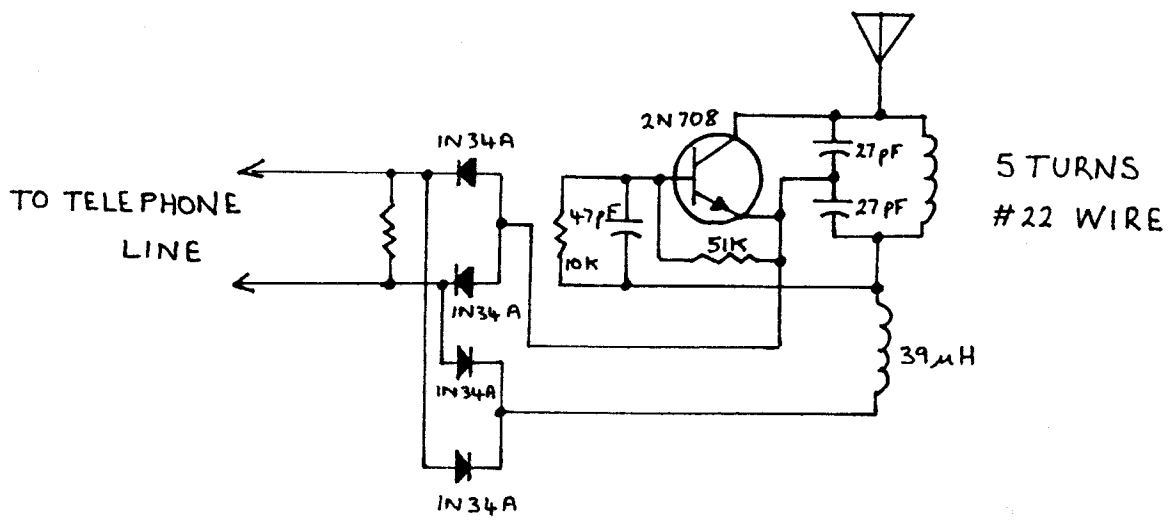


Figure 3: Telephone Taps

The induction coil technique is somewhat difficult to implement, however, because the low level magnetic field which surrounds the operating telephone line produces a correspondingly low signal level output from the sensing coil. The direct wire equipment is much easier to attach, and provides a more reliable and usable output signal, which is readily recordable. Neither of these techniques will disturb the line voltages or current characteristics and alert the target or telephone company: the induction coil does not touch the line, and therefore draws no current; the direct wire connection draws only alternating current by virtue of its capacitive connection, and therefore leaves no signature for the central office. If an improper connection to the telephone line is made; for example, if a tape recorder input were connected directly to the lines, the change in line voltages or normal audio signal could alert the telephone company or subscriber and would most likely result in poor wiretap performance because of the poor electrical match between the recorder input and the telephone line.

After the eavesdropper has successfully intercepted the telephone line's audio signals, they must be communicated to a convenient location for monitoring and possible recording. In telephone company assisted "legal" wiretapping, the preferred solution is to lease a pair of lines to carry the signal from the target lines to the listening post. This practice also allows the eavesdropper to monitor many lines, if necessary from the convenience of an office or central monitoring point. At the listening post an assortment of recording equipment and accessories are used which are described later. The properly installed direct hardwire connection is preferred over most other wiretapping techniques because of its reliability, superior performance, good quality audio, and increased level of security from detection. If not used, the reasons usually relate to the time involved for proper installation or operational restrictions. Items 1, 2 and 3 on figure 1 illustrate these methods of wiretapping.

Radio Systems. Should the eavesdropper be unable to complete the wire communications link between the target telephone lines and the listening post, a second alternative involves use of the radio tap transmitter. These devices are the same as room radio bugging transmitters except that they require no microphone, since the audio signals are already in an electrical form, and may use normal telephone line voltages for power, rather than batteries. To intercept the audio signals, the radio tap transmitter may be connected directly to the telephone lines or to an induction coil which senses the magnetic field around the wire or telephone instrument itself. Figure 4 illustrates three types of radio tap transmitter installations. The point of attachment of a radio tap transmitter is arbitrary, limited only by the ability of the eavesdropper to gain access to the telephone system, as the device may be installed within the instrument itself, anywhere along the telephone line within the building, on a telephone pole, or in the wirecloset or terminal room of an office building where many lines are joined to form a cable. Once in

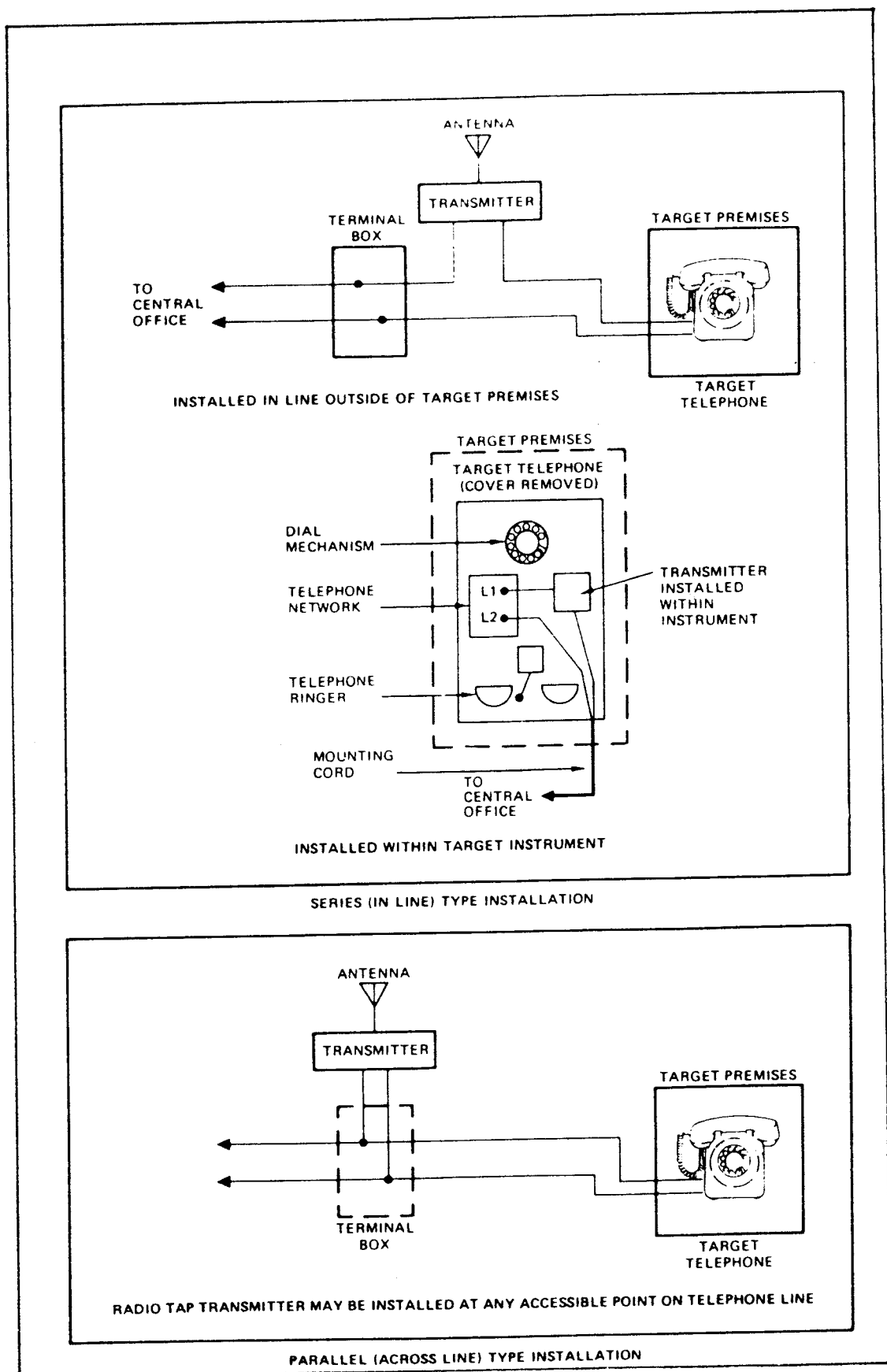


Figure 4: Radio Tap Transmitters

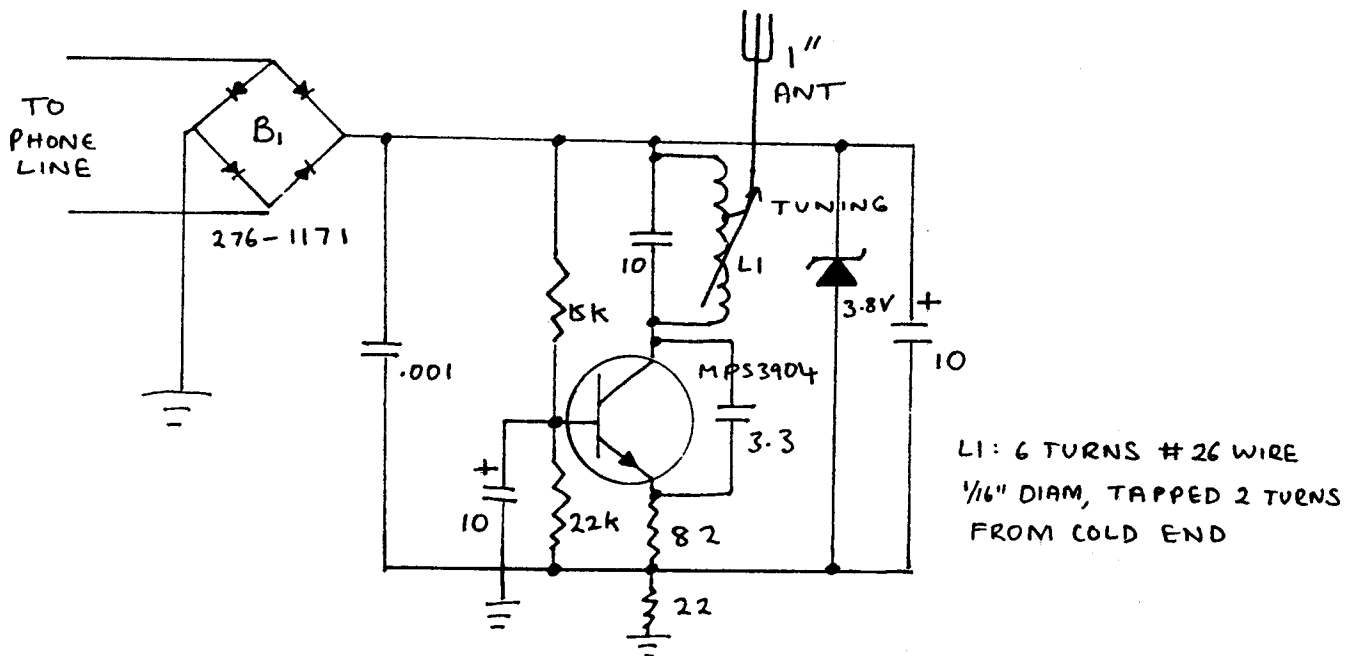


Figure 5: Telephone Drop-in Mouthpiece

place, these radio transmitters send whatever electrical signals are on the telephone line to a remote radio receiver. They are easy to install and are the preferred telephone tap method where the transmitting range is small, generally one to three city blocks and where a leased line or direct wire connection is not possible.

One very popular radio tap transmitter, the telephone drop-in mouthpiece (figure 5), is simply placed in the telephone handset after removal of the original mouthpiece unit. Many "law enforcement suppliers" offer radio tap transmitters which are intended primarily for this purpose though their attractiveness is limited because they may be readily identified through visual inspection inside the hand-set. Some mail-order sources offer an inexpensive "electronic telephone conference call monitor" which could be used as a clandestine radio tap transmitter by an individual desirous of a quick, short range, inexpensive tap. Radio devices which are installed within the target telephone require entry to the premises for implacement whereas those connected to the external lines require no entry and suggest different legal implications.

The majority of the radio tap transmitters offered commercially use conventional FM modulation, but a few use more sophisticated modulation techniques to reduce the probability of detection. Other types of modulation are discussed elsewhere. Another means of increasing the security of a radio tap operation is to locate the transmitter far enough away from the target telephone so that it is undetectable by a bugging countermeasures team, but close enough to the eavesdropper's receiving set

to provide effective operation. Installed in this manner, the radio energy emitted by the transmitter would carry the information as far as a conveniently located listening post, but perhaps not as far as the target instrument, thereby avoiding detection in the area by the security sweep team's radio-frequency (r-f) sensing equipment. The smallest radio tap transmitter offered commercially is the size of a corn kernel; "small enough to be inserted within the telephone wire sleeving". This device operates in the VHF region and, according to the manufacturer, will effectively operate over a range of up to 100 metres.

Accessories. At the eavesdropper's receiving site, the incoming electrical signals from either wire or radio transmitters are usually recorded on a conventional tape recorder for later playback. Several electronic accessories may be used which permit the eavesdropper to record the telephone numbers dialed by the target along with the date and time. These devices are commonly known as pen registers (or dial impulse recorders, also sold as "computerized phone accounting systems") and touch tone decoders. Originally designed for use with dial telephones, these devices record the telephone electrical impulses which are generated during dialling as dots on a strip of paper. The pen register operator simply counts the dots in each dial pulse group to determine the number called. Today these devices are fully electronic and present the operator with the actual number dialled, either printed on paper tape like an adding machine or in a lighted numerical display. Generally, the devices are expensive and not publically available. For the eavesdropper unable to obtain theses devices, a multispeed audio tape recorder may suffice as a dial decoder. The tape speed can be reduced after recording a telephone dialling sequence. The pulses may then be counted to determine the telephone number dialled. With touch tone phones, the peculiar tones produced must be compared with those produced by a similar phone to identify the appropriate digits.

Other accessories include two telephone line voltage activated switch devices. One is called a telephone slave, and the other is the cheesebox which is now obsolete. Usually the two wires extending from one side of either device are attached to an accessible telephone line pair. In the case of the slave unit, the second connection is made to the telephone line which is to be monitored or tapped. When the telephone number of the first line is called from any location, the slave will automatically respond to the call by connecting the two lines together, thereby permitting the eavesdropper to wiretap or remotely monitor conversations taking place on the other telephone line. These devices are used by government operatives when leased lines are not available. They effectively allow several lines to be wiretapped from a single telephone at the listening post, thereby eliminating the requirement for multiple leased lines. The telephone slave tends to be unreliable in practice, however, and occasionally will malfunction causing the eavesdropper's telephone line to be held in an open position. If this occurs, the next time the eavesdropper calls the slave unit, a busy signal is continuously

received.

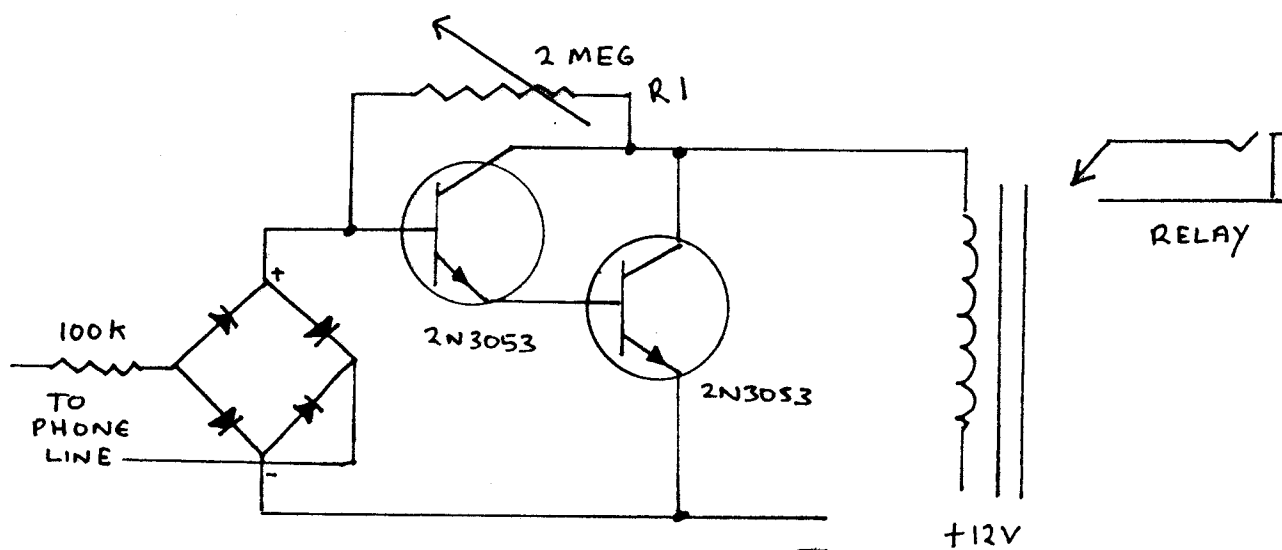
In another application, a slave type device may be connected, not to a second telephone line, but directly to a microphone and amplifier to allow monitoring of room sounds rather than telephone conversations. This procedure requires that a microphone and amplifier be installed in the target area and that an unused telephone line be available nearby for the connection. At any time, the number of the unused line may be dialed from a remote point, and the eavesdropper will be connected automatically to the microphone to monitor the premises. Some devices offered for "law enforcement use" contain the slave type switch and microphone prepackaged in a standard telephone connector block.

The cheesebox is similar to a slave in operation but, instead of connecting one telephone line to another for eavesdropping purposes, it connects the two lines and permits two-way conversation between the parties to prevent call tracing. However, little use is currently found in any sector (private or government), since the more efficient, modern call forwarders which are discussed in the following paragraph can be made to serve a similar purpose.

A legitimate and widely used telephone accessory is the call-forwarder or re-dialer. The device is connected between two existing telephone lines, and a telephone number is entered electronically into the unit. When a call is received on one telephone line, the unit automatically dials the internally stored second number to reach the desired second telephone. These devices are being increasingly offered by telephone companies and are used by doctors, executives, and others who wish to receive incoming calls at a more accessible number while away from office or home. When used in a business environment, these devices frequently have provisions for third party monitoring.

Voltage and voice actuated automatic switching devices are widely used in illegal audio eavesdropping systems. Their function is to sense the changing voltages or audio signals on a telephone line caused by use of the telephone, and thereby automatically turn recording equipment or radio transmitters on and off. This is necessary to conserve recording tape or avoid unnecessary radio transmissions. Voltage actuated devices are readily available as components of some automatic telephone answering devices or telephone secretaries.

The audio amplifier (figure 7) is a fundamental tool in all communications activities. It is on the eavesdropper's list of equipment and is used not only in telephone line tapping but also with microphone systems. Basically, amplifiers serve to increase the relatively small audio signal level which exists on telephone lines, or at the output of a microphone, to a level which is strong enough to be used in the intended manner. An additional amplifier is usually not required for use with a good quality tape recorder because of built-in amplifying circuitry. Audio amplifiers are also used in countermeasures inspections for eavesdropping devices. These small amplifying units with built-in speakers are available from general electronics stores, but do require some type of matching



ATTACH RELAY TERMINALS TO TAPE RECORDER 'REMOTE' JACK.
ADJUST R1 SO THAT RELAY CLOSSES WHEN PHONE IS IN USE

Figure 6: Automatic Tape Recorder Starter

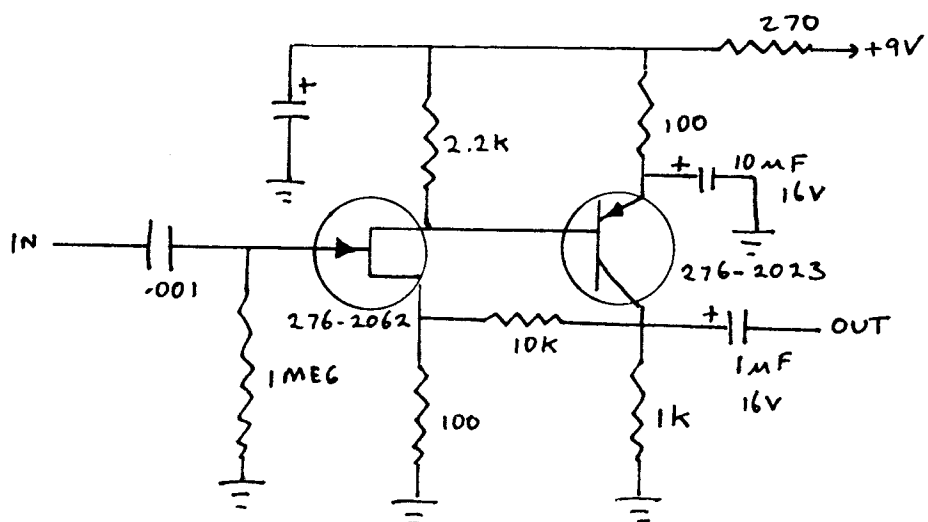


Figure 7: Audio Amplifier

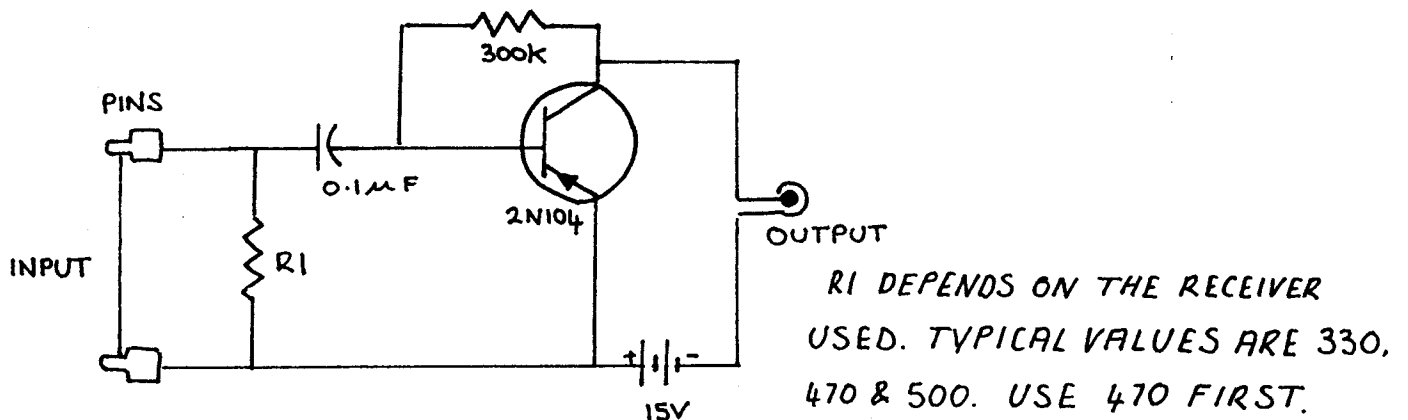


Figure 8: Headset Booster

circuitry for use directly on a telephone line.

Telephone Eavesdropping. The previous paragraphs discussed those procedures and devices used by an eavesdropper for telephone wiretapping, which is limited to the monitoring and recording of actual telephone conversations. This section describes several other devices and techniques which cause separate portions of the telephone instrument to act as part of a room eavesdropping system. Items 5 through 7 in figure 1, the telephone instrument diagram, show devices discussed in this section which accomplish this purpose. None are intended for the reception of telephone conversations.

Infinity Transmitters or Harmonica bugs. The most widely publicised room eavesdropping device that uses the telephone system is the infinity transmitter or harmonica bug. The name infinity transmitter is derived from the original manufacturers claim that it could eavesdrop on room conversations from an "infinite" distance by using the telephone system wires. These devices are not really transmitters at all but are tone controlled switches usually coupled with an audio amplifier and microphone. The tone switching mechanism in the transmitter is designed to activate the microphone when it receives an electrical signal or audio tone of a specific frequency over the telephone line. Originally this audio frequency or tone was usually about 440 Hz (a "C" note on a harmonica); because of this the popular name "harmonica bug" was derived.

To operate the infinity transmitter, the eavesdropper dials the target telephone and before the telephone rings, the harmonica is blown or a tone beeper is sounded into the eavesdropper's telephone mouthpiece. (Newer devices are available which use multiple tones to activate the transmitter, thus making detection by sweep teams more difficult.) On the target telephone, the infinity device required receives the audio tone and

switches the device to answer the target telephone electrically rather than physically. The target telephone should not ring if the eavesdropper is quick enough with the activation signal and if the telephone system itself is designed so that the signal reaches the target instrument without delay. If the target instrument does ring, the eavesdropper may merely wait for the subject to answer, pretend to have dialled the wrong number, and when the target handset is returned to the cradle, quickly activate the infinity device and monitor the room sounds. If the subject uses the telephone to make a call, the eavesdropper hangs up his own telephone and the listening device is disconnected.

These devices are only effective on older, crossbar-type equipment, not on newer, electronically switched systems (ESS). This is due to the fact that in ESS systems there is no complete audio path between two parties until the recipient of a call actually answers the telephone. This eliminates the possibility of transmitting a tone to a "bug" before the ring voltage is sent: there is simply no path for this tone.

Crossbar-type equipment is distinguishable by the fact that there is a delay before the waiting tone returns after the hook-switch connection is broken (by depressing the buttons on the top of the phone.) ESS equipment yields no such delay, and allows call-forwarding and other services not possible with crossbar equipment.

Other systems, be they electronically switched or not, may also operate differently, so that in some the audio connection is made before the ring voltage is sent and infinity devices will work, and in others the connection is not made at that point and such devices will prove ineffective. These differences are encountered from country to country and locale to locale, and therefore mandate tests by the eavesdropper.

Today infinity devices are offered for sale to "law enforcement personnel" in small, easily installed electronic modules; they are offered to the public as well, but not as eavesdropping tools. In many cases, they are advertised as an inexpensive audio burglar alarm that allows the home owner to call his residence telephone while away on a trip and listen for burglars. Infinity devices are installed by entering the premises and making a wire connection to the telephone lines at any point in the area to be monitored, a procedure clearly described by the manufacturer's instruction sheet. The point where the connection is made depends upon the eavesdropper's intentions; it may be installed near or inside the telephone instrument, or in another room apart from the instrument where the line passes on its way to exit the building. Once in place, the device monitors all nearby room conversations when it is activated.

The major drawback to successful use of these devices occurs because the telephone line appears to be in use to the telephone company's automatic sensing equipment, and all callers to the target telephone number receive the normal busy signal while the infinity device is in use. This may quickly raise questions and alert the subject that something unusual is affecting the telephone line.

Further, the infinity type of device can be easily detected while in

operation. Since the telephone line voltage changes when the telephone is used, an operating infinity device causes the voltage to behave in a similar manner. By measuring this voltage change, technicians can determine if an infinity device is active, and by monitoring the line with other audio sensing equipment, may listen to the same audio signals the eavesdropper is receiving. Finally, the eavesdropper has no way of determining in advance if any interesting conversation is transpiring in the target area, and the target premises must be repeatedly monitored, causing suspicious, lengthy or repeated telephone line use.

Listen-Backs and Keep-Alives. Two devices which are modifications of the infinity transmitter are known as listen-backs or keep-alives. These devices contain simple electronic components available through conventional electronic retail outlets. They are not tone activated like the infinity device and do require that the subject telephone be answered to operate. These devices must be installed across the hook-switch within the instrument itself and operate by holding the line open between the eavesdropper's telephone and the target telephone after the call is completed and the target telephone handset is returned to the cradle. The target instrument is maintained electrically off-hook by the listen-back device and the eavesdropper may listen with an audio amplifier to conversations taking place in the vicinity of the instrument. To disconnect the device the eavesdropper hangs up, causing a line voltage change which disconnects the device. These devices suffer from the same disadvantage in use as infinity transmitters and, in addition, installation within the telephone instrument may be difficult. They are smaller and less expensive, however, than the harmonica bug because they contain fewer parts. For this reason they may be difficult to identify as eavesdropping devices prior to actual installation within the target telephone.

On-Line Microphones. If The eavesdropper has access to a telephone line that passes through the target premises, a device known as an on-line microphone may be used as part of another type of monitoring system. The basic device consists of a microphone, miniature audio pre-amplifier, and matching circuitry. It is connected directly across the telephone wires in the target premises and cannot be dialled or activated from a remote telephone to eavesdrop on the premises. The intercepted radio signal is transmitted only over the unused telephone line pair to the listening post. They are therefore severely range limited, since these signals will not pass through the telephone company's switching exchange. This device, unlike the infinity transmitter and listen-back devices, does not disrupt incoming and outgoing calls; however, because the device is not generally remotely switchable, the intercepted audio signal may be present on the unused wires leaving the target premises and may be detected by a competent countermeasures sweep.

Telephone Modifications. In the earlier description of the standard telephone instrument it was pointed out that a telephone consists of an earpiece, mouthpiece and associated circuitry separated from its transmission lines by the hook switch. The eavesdropping devices discussed to this point make use of the telephone lines and, at the same time, generally exploit the normal operation of the complete system. But an important feature of the telephone instrument of interest to the eavesdropper is the hook switch within the instrument itself. If the eavesdropper can somehow short-circuit or bypass this switch, the telephone handset will act as an open room microphone.

The process of shorting or bypassing the hook-switch in a manner that does not affect the normal operation of the telephone, but causes the unused telephone to become a microphone is known as telephone compromising. It is accomplished by the eavesdropper by producing any of numerous electrical circuit changes inside the telephone.

The electrical symbols shown in figure 1 above location S2, the hook-switch, indicate several possible telephone instrument modifications and are but a few examples of the many changes that are possible. The objective of these changes is generally to activate the telephone's carbon mouthpiece by allowing a small, nearly undetectable amount of direct current to flow through the instrument.

Occasionally, the telephone's earpiece may be made to serve as the eavesdropping microphone because of its magnetic nature which permits it to function not only as an earpiece, but also as a microphone. If the eavesdropper elects to use the earpiece, the electrical signals must be amplified more than signals from the mouthpiece to compensate for its lower level signal output. Once the room audio is passed through the unused instrument into the outgoing lines, the eavesdropper may intercept it only at a point between the modified target instrument and the first telephone company switching exchange. At this interception point the audio information may be monitored by earphones, recorded, or transmitted by radio to a more remote listening post. In addition to the modified telephone instrument, the eavesdropper must use other electronic devices to complete the operational system. Not only must the intercepted room audio from the lines be amplified but also ring voltages from other callers, which are much larger in amplitude than the audio signal being monitored, must be filtered. The electronic devices necessary to accomplish this filtering, detecting and switching process are relatively unsophisticated and could be reproduced from easily obtainable electronic components. The only remaining consideration is that care be taken not to disturb the normal quiescent electrical status of the telephone line. To alter or disrupt these characteristics would cause the telephone company to investigate the excessive current drains, voltage changes, or line noise and increase the possibility of discovering the eavesdropper's activity.

The compromise of a telephone instrument is one of the few eavesdropping practices which generally requires technical skill and a thorough knowledge of the telephone system for successful implementation. This

fact, plus the operating range limitation and the difficulty in selecting the specific line pair of the target instrument from the maze of other wire pairs, causes this method of eavesdropping to be unattractive to many eavesdroppers. Only one commercial manufacturer offers the complete electronic telephone compromise system in a single package to "law enforcement agencies".

The modification of single line instruments is far easier than modification of the standard five-button office telephone for two reasons. First, the internal complexity of the multi-line system requires additional skill and experience beyond that required for single line compromise; second, the rotary type line selection switching, commonly found within the office areas equipped with multi-line instruments prevents the selection of a specific line pair from outside the area. This latter difficulty essentially eliminates the probability that a single, multi-line target instrument would be compromised for an external audio penetration, but leaves some possibility for a penetration from within the internal office switching network, that is, between two instruments sharing a common line extension. Use and knowledge of this eavesdropping technology has been understood for years but only recently has become of interest to the non-government eavesdroppers.

Radio Frequency Flooding. An occasional newspaper article mentions a highly sophisticated technique by which a normal telephone can be converted to a room listening device. This esoteric technique is called radio frequency flooding. Although reported to be a threat, it is generally known only to sophisticated electronics experts, is extremely difficult to implement, very range limited and requires an abundance of expensive electronic equipment. As it has little or no application, it will not be discussed here.

Microphone Systems

Use of a concealed microphone is the oldest of all electronic eavesdropping methods and is still the most reliable approach to clandestine monitoring of room conversations. The advantages over other methods include the system durability, security and limitless operating life. Properly installed, the "mic and wire" system with switching actuators and several well positioned microphones can be remotely controlled by the eavesdropper to allow monitoring of different, selected areas. Since the wire portion of the system is usually attached directly to a tape recorder or an audio amplifier (headphones may be used for direct monitoring), there is no need for radio transmitters, receivers or other costly electronic equipment. All components required for the basic system are readily available and offered for sale without restriction.

The system performs two functions for the eavesdropper. The microphone converts room sounds into electrical signals, and the wires carry these signals to the eavesdropper. The microphone is usually supplied with its power from the monitoring post, via the same wires that carry the

intercepted audio signal to the eavesdropper. These wires could run for several miles, and a distinct advantage is gained by the remote power source, in that once the system is installed there is no need to risk entry to the target premises for the purpose of changing batteries. In addition, this permits the eavesdropper to disconnect the power supply and reduce the possibility of detection by a countermeasures team's electrical analysis of the wires exiting the premises. For operation over the several mile range, special wires, pre-amplifiers, and line drivers located near the microphone may be required. The following sections describe several

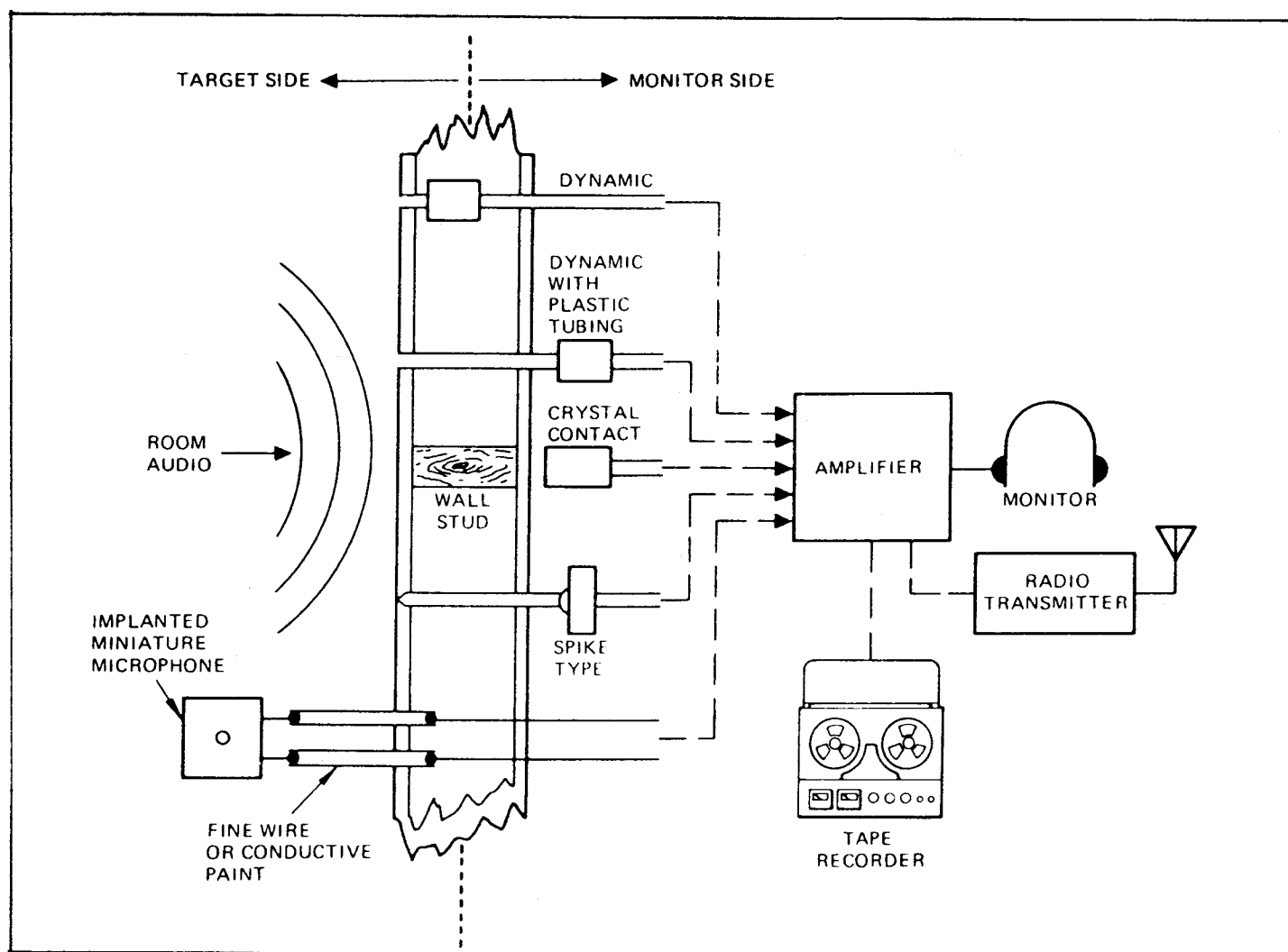


Figure 9: Various Microphone Types and Methods of Covert Installation

microphone types available today and their application to audio surveillance.

Types of Microphones. The microphone is by no means limited to use with wire systems. The types of microphones described in this section are used with radio transmitters, infinity transmitters, tape recorders and other devices which receive and convert sound to an electrical signal. This point should be kept in mind as the different types are discussed.

Carbon Microphones. The original microphone invented by Alexander Graham Bell in 1876 was a carbon microphone. Its durability, reliability, ruggedness and resistance to changes in humidity and temperature still see some use among eavesdroppers, however it is gradually losing favour to the more versatile condenser microphones now available. Nevertheless, it is still used today as the mouthpiece for many telephone instruments (one reason for its enduring popularity). The carbon microphone suffers somewhat as an eavesdropping device because it needs power to operate. In some installations the power can be supplied from the listening post through the same wires which carry the audio signal but this inconvenience will generally limit the range between the eavesdropper and the target area. This characteristic also prevents the carbon microphone from being used in small battery powered radio bugging transmitters where an attempt is made to keep power consumption low to extend the device's operating life. The physical characteristic that detracts from its usefulness in an eavesdropping system is its size; it tends to be larger than other types of microphones and thus less easily concealed.

The carbon microphone operates in the following manner. A small voltage, perhaps the amount supplied by a single flashlight battery, is connected in series with the terminals of the microphone through a long pair of wires. A few milliamperes of direct current will flow from the battery down one wire, through the microphone and back to the eavesdropper's equipment on the other wire. While this direct current is flowing, the microphone modulates the current in a manner proportional to the sound it receives in the target area. This modulated electrical signal is then separated at the listening post and actively monitored or recorded.

Magnetic Microphones. The magnetic or dynamic microphone has characteristics which make it very attractive as an audio eavesdropping tool. These microphones require no power to operate, are usually quite small and convert sound into electrical signals by the movement of a small coil of wire near a permanent magnet. This action generates small electrical signals in the coil proportional to the coil movement caused by the sound vibrations striking a thin diaphragm which is physically connected to the coil of wire.

For eavesdropping purposes, this ability to generate the required electrical signal from room sounds is a very important feature. This means that no power for the microphone is drained from the battery of a radio transmitter, recorder, or other powered device to which it is attached. In

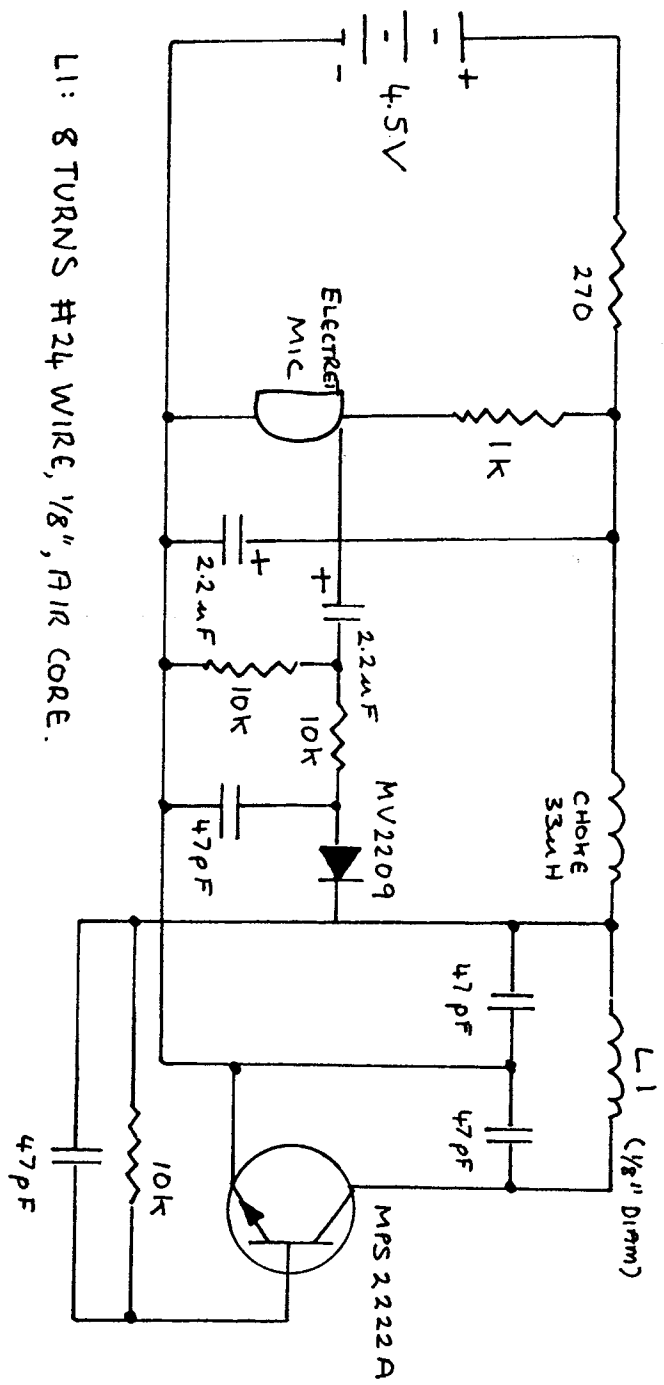
the "mic and wire" system, however, this feature is not of value since the electrical signal generated is very small and will not travel very far over a wire without the addition of an amplifier. Nevertheless, magnetic microphones are used in eavesdropping because of their small size, low cost and high sensitivity. Figure 9 illustrates installation techniques for a variety of microphones used in audio surveillance and one method of "painting" a pair of wires using silver paint. This silver paint is electrically conductive and will carry the microphone's audio output signal to the eavesdropper in the same manner as a wire pair. It can be constructed by grinding copper pieces into powder, adding them to an adhesive (preferably the ethyl-based kind purchasable at radio stores), running this compound from a to b then painting over it.

The dynamic microphone is frequently offered (by "law enforcement equipment suppliers") in pre-packaged concealments, such as in cuff links and eye glasses for use with body-worn recorders or radio transmitters, and in electrical wall sockets or appliances for room monitoring installations. These concealed microphones are nominally priced, and a few contain built-in amplifiers to increase the amplitude of electrical signals produced by the microphone for transmission over longer wire paths. Other types of microphones can be easily concealed in these same objects, but generally, the dynamic device is chosen because of its relative advantages over other types.

Speakers. The primary function of a speaker is to generate sound from applied electrical signals rather than sense sound and generate an electrical signal output. The ordinary permanent magnet (PM) speakers, commonly used in portable radios, walkie-talkies and stereo systems can be made to serve as an eavesdropping microphone as illustrated in Figure 10. The PM speaker is structurally similar to a dynamic microphone with a coil of wire positioned in a magnetic field. When used as a speaker, electrical current is passed through the coil which vibrates the speaker to produce sound. Most of these speakers show varying degrees of reciprocal performance and can therefore be used as microphones. When acoustical energy impinges on an unused speaker cone and vibrates the coil of wire in the permanent magnet field, small amounts of electrical energy are produced which can be transmitted by radio or over wires to a listening post. This fact is frequently overlooked by many countermeasure sweep teams, and radios, stereo speakers, public address systems and intercom systems frequently go unchecked.

A method for using a speakers as an eavesdropping transmitter is shown in figure 11.

Condenser Microphones. The condenser microphone has gained some popularity in recent years because of its adaptability to high fidelity applications. These microphones are electrical capacitors which, when impacted by acoustic energy, change their electrical characteristics by changing the capacitance of the microphone circuit. These microphones exhibit good response in the spectrum of 30 to 18 000 Hz, the full range



L1: 8 TURNS #24 WIRE, 1/8", AIR CORE.

FIGURE 10: MINIATURE DEVICE

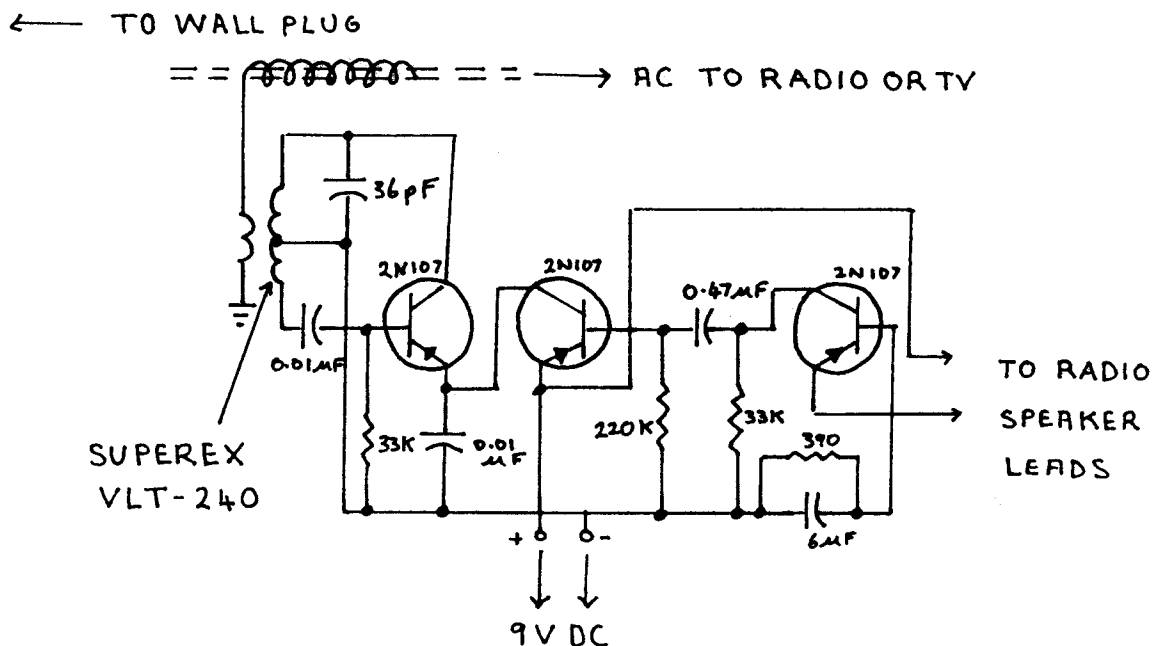


Figure 11: Use of a Speaker as a Microphone.

of human hearing, and are now generally used for audio surveillance because of their small size and excellent frequency response.

Electret Microphones. This non-magnetic device is extremely small in size, and has high sensitivity and good frequency response. It is similar in construction to a capacitor type except that a voltage charge is permanently stored internally, and it is the vibration of this charge in response to the room audio which produces the electrical output signal. The electret rivals the magnetic microphones in eavesdropping applications, since it exhibits most of the beneficial characteristics of the magnetic unit and has the advantage of producing larger electrical signals with its built in pre-amplifier.

Special Purpose Microphones. Performance improvements can be made to the basic microphone to increase its ability to receive low level sounds. Many manufacturers offer different devices which contribute to this enhancement and, therefore, are of interest to the eavesdropper. These primarily include directional microphones such as shotgun or parabolic devices and pneumatic cavity or contact microphones, designed for listening through windows and walls. Each of these is discussed in the following paragraphs.

Contact, Spike and Pneumatic Microphones. Figure 9 illustrates the application of the contact or spike microphone, a device long popular with eavesdroppers. This microphone contains a special crystal which, when

slightly compressed, will produce a very small electrical signal. If it is placed against a vibrating wall or window pane or attached to a rigid probe which is touching one of these vibrating surfaces, the crystal will produce small electrical signals which correspond to the vibrations. If these vibrations are caused by room conversation sounds, the electrical signal will correspond to those sounds. The signals generated in this manner are small and are of sufficient strength to travel far over wires. These devices tend to be fragile and are not able to stand temperature, shock and humidity changes, but are sometimes used today in illegal eavesdropping activities.

Contact microphones may be improvised from electric guitar microphones, which are designed to pick up the vibrations of the strings without the use of a resonating cavity. This makes them ideal for sensing the small vibrations transmitted through walls.

Spike microphones can be constructed using a wall stud and microphone (as shown in figure 12)

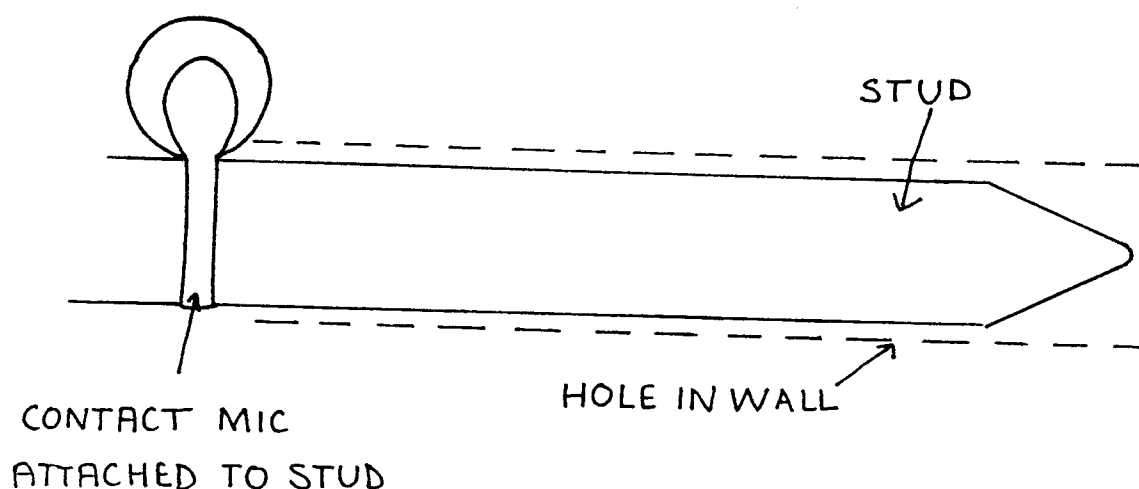


Figure 12: Spike Mike

The pneumatic cavity microphone is an electronic version of the glass tumbler against the wall, historically recognised as one method of monitoring adjacent room conversations. This microphone is substantially superior however and operates by using a specially constructed small cavity which in general is highly responsive to surface vibrations at the audio frequencies found in human speech. This cavity is used in conjunction with a conventional microphone to enhance its performance and force its output to correspond to wall surface or window vibrations rather

than a direct sound input. Several manufacturers offer these microphone systems publically as electronic stethoscopes or cavity microphones, but few eavesdroppers use such technology.

Shotgun and Parabolic Microphones. The shotgun and parabolic type devices are used by the entertainment and sports industries and occasionally by law enforcement personnel with varying results. The parabolic microphones operate by concentrating the audio energy gathered over an area the diameter of the parabolic reflector, typically 1.5 to 3 or 4 feet, onto a conventional microphone. The large area of the reflector plus its shape causes audio energy received at the microphone to be much greater from one direction than that which would be received by the microphone alone. These devices, under ideal quiet conditions can retrieve normal conversation from a distance of 300 feet, but in practical use are somewhat limited because of background interference such as wind and ambient noises. Some audio equipment companies offer parabolic microphones on a rental basis for \$15.00 per day or \$30.00 per week, as well as the briefcase to carry all the equipment, recorders and audio amplifiers.

Parabolic microphones can be improvised by boring a hole in the centre of a parabolic (or near-parabolic) salad dish, made from metal or plastic. An ordinary mono microphone can then be placed in this hole, connected either to a tape recorder (the most practicable alternative), a headset or an amplifier.

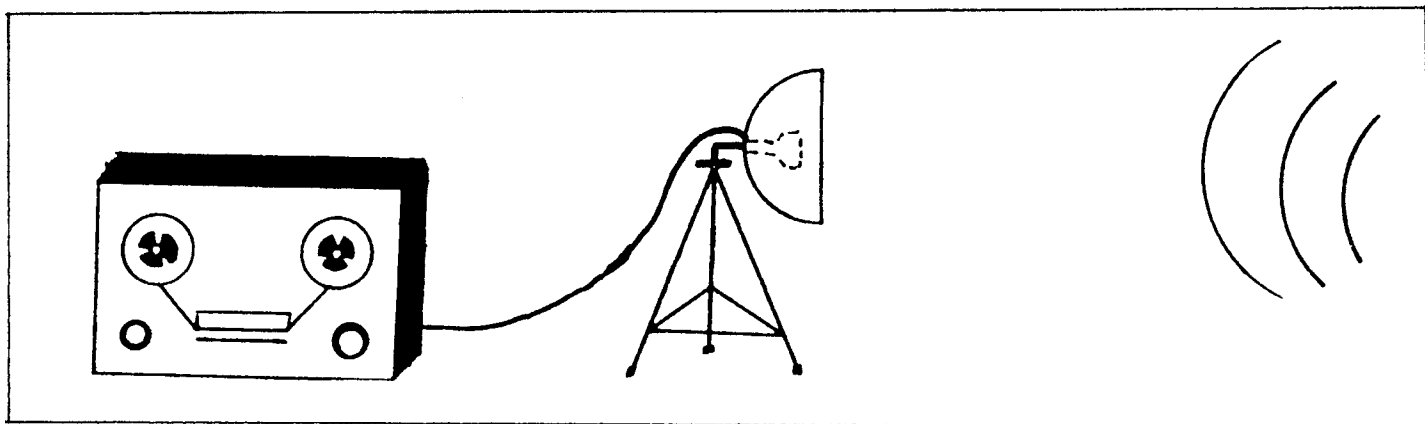


Figure 13: Parabolic Microphone.

From a practical viewpoint, the parabolic microphone is only usable

where its large size would not be alerting to the target and where there is a free audio path between the target and the surveillance system. One conventional scenario satisfying these limitations would be the night time operation in an open field or park with the target engaged in a conversation in an extremely quiet environment.

Another directional device is the shotgun microphone which shares many directional characteristics with the parabolic unit. It receives audio from a specific direction through the use of an arrangement of various length tubes, ranging sometimes from 5 centimetres to 1.5 metres. Sound travelling axially (i.e. from the direction of interest) enters each tube in decreasing order of size, maintaining the original phase relationship. Thus at the microphone, signals from all tubes are in phase leading to good signal pickup.

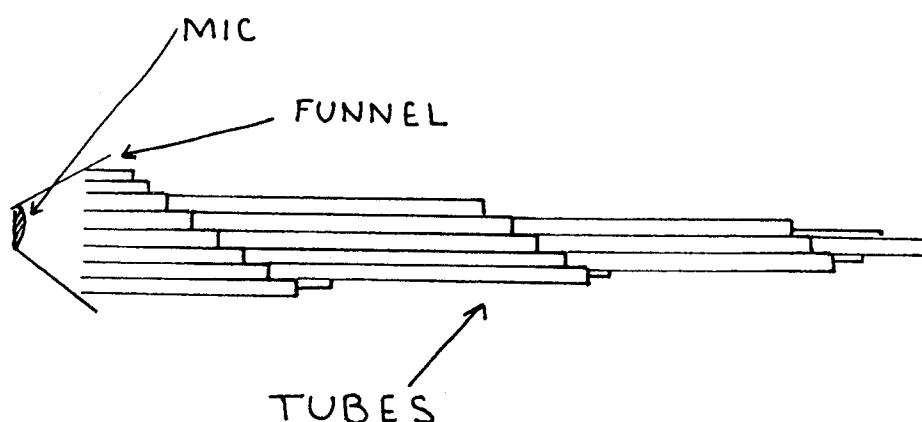


Figure 14: Shotgun Microphone.

Signals arriving from sources away from the axis will enter all tubes at the same time. However, as each tube is of a different length, the audio signals will be of many different phases when they finally reach the microphone, leading to considerable cancellation. In this way, extraneous signals are filtered out, leaving high quality audio from the desired direction.

A shotgun mic may be constructed from pieces of aluminium tubing (such as old TV antennas), cut to different lengths and glued to each other such that the shorter pieces lie on the outside of the device. The lengths of the pipes should range from about 3cm to 1m, and increase in increments of 2-5cm (see diagram). A funnel can then be fixed at the receiving end of

the device, and a crystal microphone element placed in the centre of the funnel. The audio signals can be fed to an amplifier or FM transmitter.

These units tend to be somewhat bulky and may be several feet in length, requiring a tripod or other fixture to hold them in alignment with the target. They must be used in an open environment much the same way as the parabolic device and tend to be slightly more directional and therefore possibly more speaker selective. Commercial shotgun microphones can be very costly but they do perform fairly well over short ranges and in most cases are superior to the parabolic microphone.

Radio Eavesdropping Devices

Radios are electronic devices which transmit or receive radio energy to convey information. The device which transmits or sends this energy is the transmitter, and the device which detects or receives this energy is the receiver. The radio transmitter accomplishes two functions: it generates a continuous radio signal at one selected operating frequency and it modulates this frequency with audio signals provided to it by a microphone, amplifier, and modulation circuitry. The resulting electrical energy contains both the audio and high frequency radio signals and is radiated from an antenna. This energy may be sensed by the companion radio receiver which demodulates it, leaving only the audio which is amplified sufficiently to operate headphones or a speaker.

The miniature radio transmitter and its companion receiver are the basic elements of a radio eavesdropping system. Characteristics of this system such as power, frequency, and modulation determine performance in an actual operation. This section reviews characteristics of devices which are used for this purpose.

Inexpensive Devices. Inexpensive transmitter devices cannot be clearly labelled as primarily useful for eavesdropping or bugging. Because of this fact, they are easily obtainable from many sources, including hobby stores, audio electronics and communications equipment outlets, and mail order houses. Due to this availability, they are the most widely used eavesdropping devices in the private sector. This group of devices includes wireless microphones, baby monitors, wireless intercoms, and telephone conference monitors, all of which are offered for sale at prices of \$5.00 to \$20.00.

These devices are relatively small, crude from a technical standpoint, and they will not operate over very long distances. The transmitter power output is generally controlled by Department of Communications (DCC) regulation, and their frequency of operation is always in or very near the commercial AM or FM broadcast bands. Devices of this nature tend to perform unreliably, and frequency instability is a common problem requiring the eavesdropper to retune the receiver continuously to maintain reception. Most devices may be easily altered by the eavesdropper to improve performance or transmission range. The wireless microphone

transmitter, the most popular of these inexpensive devices, is described in the following paragraph and is followed by a brief discussion of devices which are easily fabricated by the technically skilled eavesdropper.

Wireless Microphone Transmitters. Many transmitters are sold commercially, most operating on the AM or FM broadcast bands. These are sold as "baby nurse transmitters", "FM wireless telephone transmitters" "AM wireless telephone amplifiers", or simply "wireless microphones".

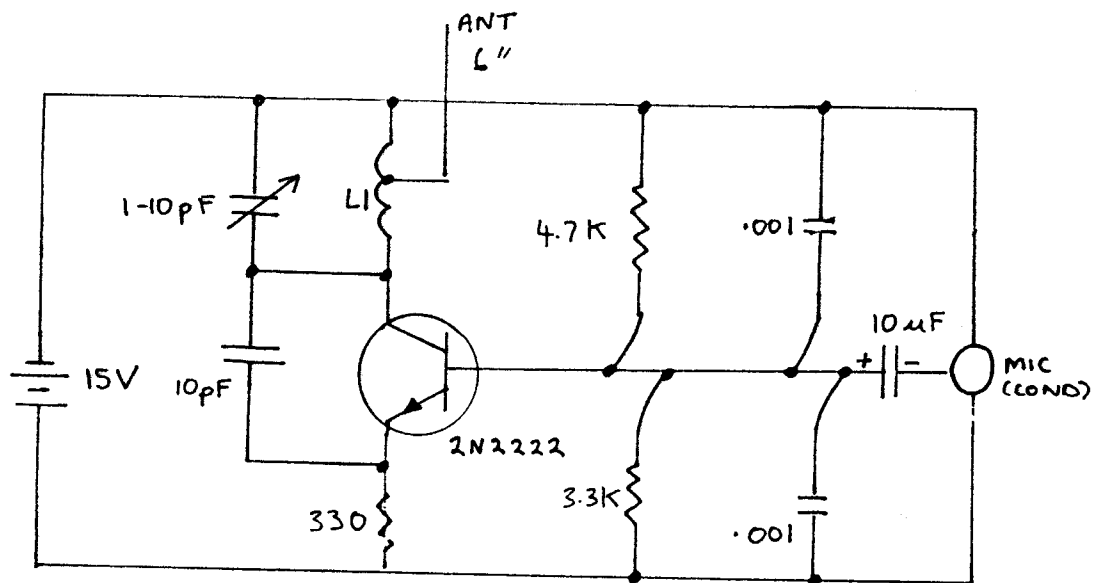
Their usefulness as eavesdropping devices can be significantly enhanced, however, by lengthening the antenna or adding another battery in series for greater range. Another modification is to change the frequency until it is outside the broadcast band to prevent accidental detection. Any of these procedures are well within the capability of an eavesdropper with very little technical skill.

Fabrications. For the more technically inclined eavesdropper, unable to buy devices legally, there is a wide choice of semi-completed devices or schematics which provide better quality and a more sophisticated end product than those just described.

The necessary electronic parts or preassembled modules can be obtained from many television repair shops or electronic equipment suppliers. Using these aids and equipment, the eavesdropper can build devices similar to those offered to law enforcement officials. Even the legitimate law enforcement suppliers frequently use these preassembled electronic modules, such as r-f oscillators, modulators and amplifiers, to fabricate a desired eavesdropping device. The individual who elects to develop quality eavesdropping transmitters requires a considerable amount of electronic equipment which can be quite costly; therefore, this process is rarely undertaken.

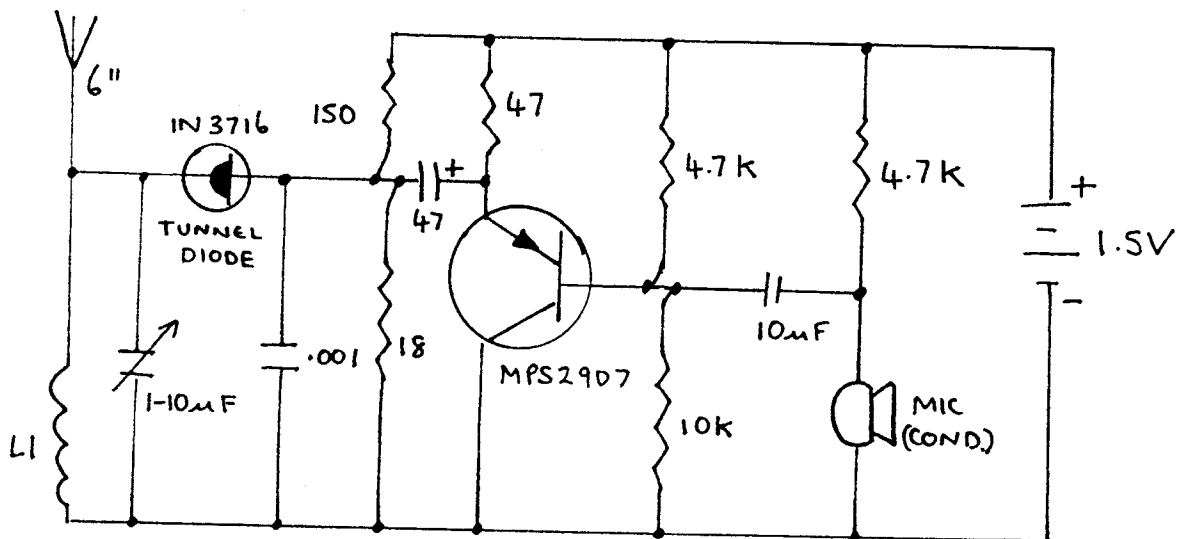
Drop Transmitters. The battery powered room transmitters are generally used by government agencies for eavesdropping operations where a quick installation is required. These devices are known as drop or quick plant transmitters and always have a finite operating life which requires that they be regularly retrieved for battery replacement. They are also for one party consensual monitoring. Several manufacturers offer used as body transmitters for security or protection purposes as well as preconcealed transmitters already packaged into objects such as ashtrays, picture frames, pen and pencil sets, and cigarette lighters. A discussion of these battery powered radio devices follows.

Miniature Devices. The smallest commercially produced transmitters identified in this study are manufactured in Europe and, as described by the manufacturer's catalogue, are the size of a corn kernel, without microphone or battery. A unit sized to fit inside a pen can be constructed as shown in figure 20.



L1: 4 TURNS #20 WIRE. CHANGE TURN NUMBER TO TUNE. DIAMETER 2.5 MM.

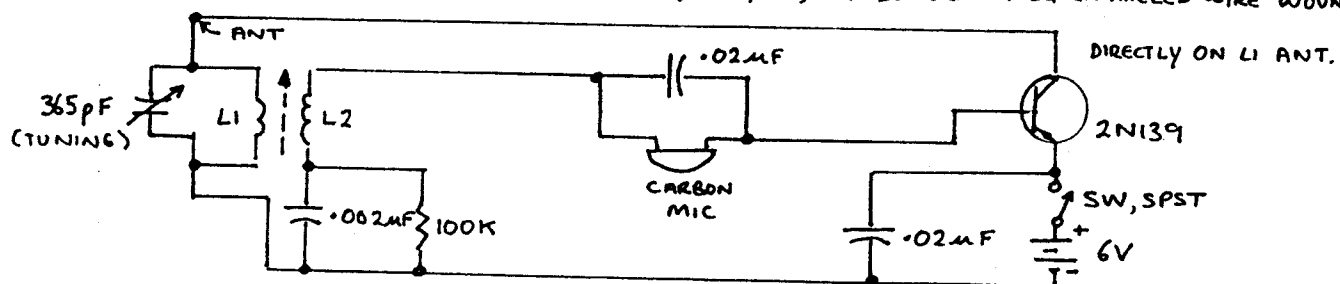
L1: 4 TURNS #20 WIRE, 2.5 mm DIAMETER.



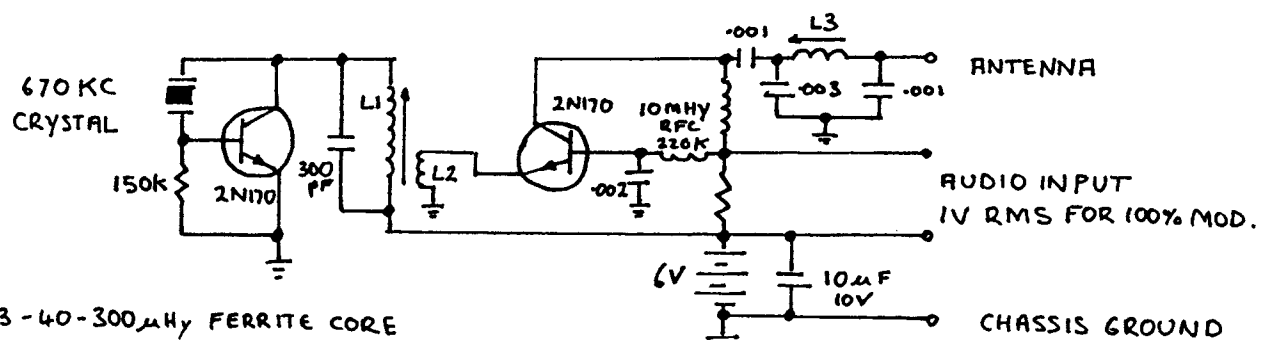
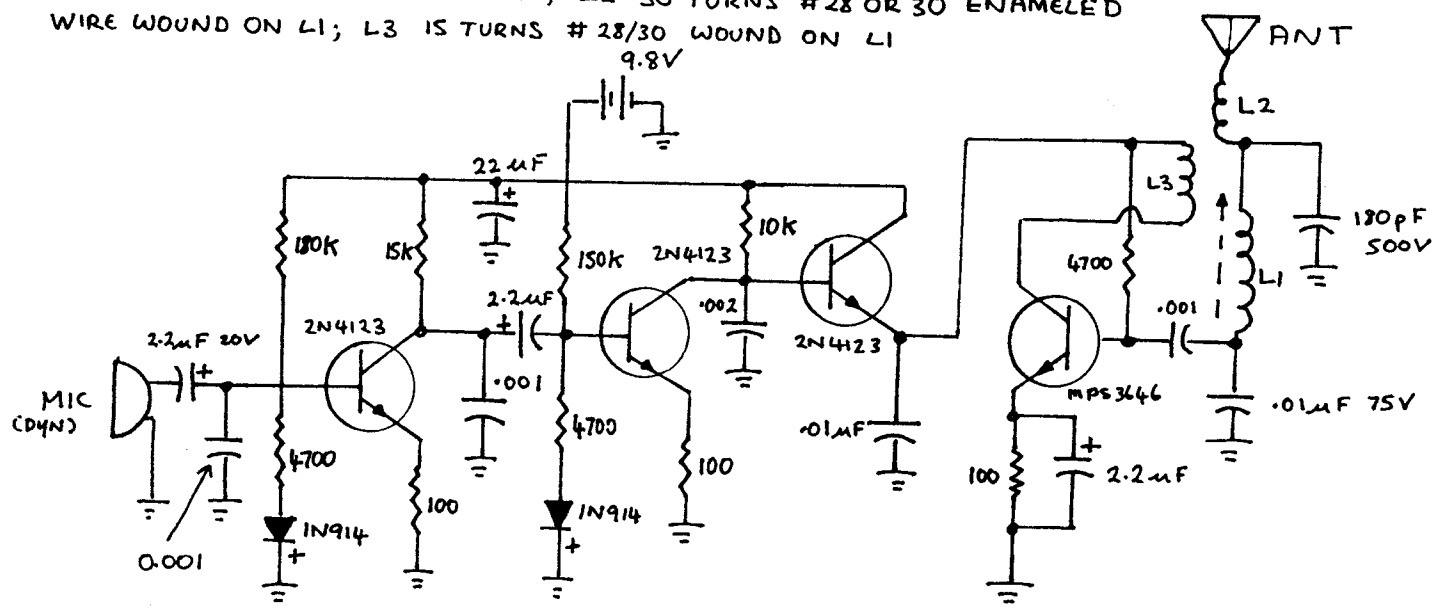
Figures 15 and 16: FM Wireless Microphones

IN ALL CASES TUNE TO LOW END OF THE AM BROADCAST BAND

L1; # 7/4 BILDEN LITZ WIRE WOUND ON 7"x0.33" FERRITE ROD, 1 LAYER, L2 36 TURNS # 24 ENAMELED WIRE WOUND



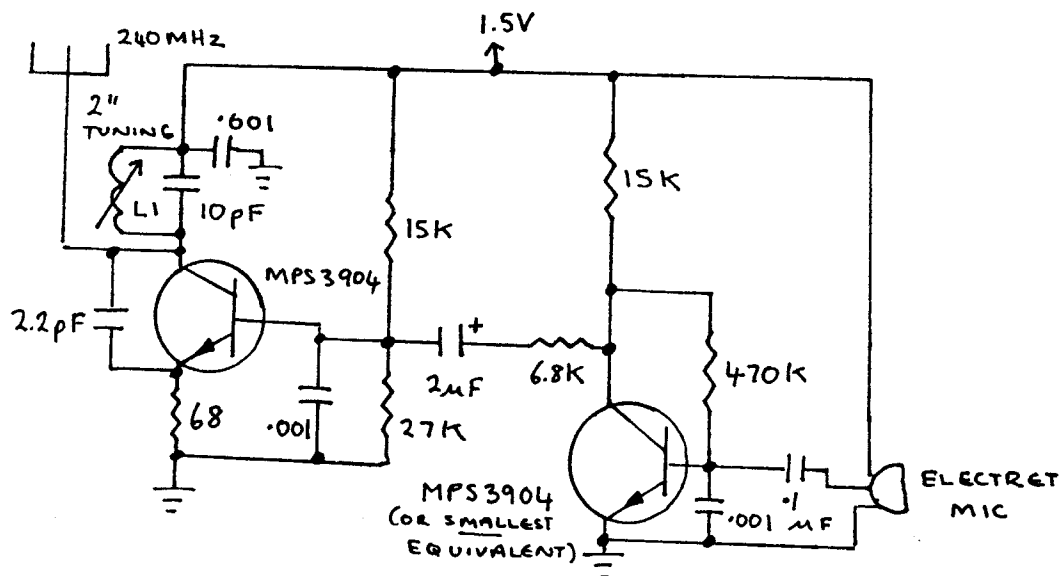
L1 HIGH Q FERRITE ANTENNA COIL; L2 30 TURNS #28 OR 30 ENAMELED WIRE WOUND ON L1; L3 15 TURNS #28/30 WOUND ON L1



L1, L3 - 40-300 μ H, FERRITE CORE

L2 - 8 TURNS #22 WIRE WRAPPED AROUND BOTTOM LI

Figure 17 and 18: AM Wireless Microphones.



L1: 3 TURNS # 22 WIRE, 1/8" DIAM.
ADJUST TURNS FOR FREQUENCY

Figure 20: Miniature Device

An operational procedure which is popular among many eavesdroppers is known as "snuggling". Regardless of the radio device power, frequency, modulation, or size, an additional level of security can be provided by carefully setting the frequency of the eavesdropping transmitter adjacent to that of a large, high-powered radio station. This is especially useful when using devices which transmit in the commercial FM broadcast band. By setting the transmitter frequency in this manner, the signal in most cases cannot be received by a standard broadcast receiver. The AFC (automatic frequency control) circuit of a standard receiver causes it to automatically select the stronger of two signals and reject the weaker of the two. The eavesdropper must use a modified broadcast receiver which can select the weaker signal.

This is an example of the more sophisticated technology available, but one which is beyond the capabilities of most eavesdroppers due to high cost and complexity. The pulse code or digital process is used occasionally in secure governmental communications systems, since digital signals can be easily scrambled or encrypted.

Carrier Current Devices. Below the AM commercial broadcast region of the radio frequency spectrum is a region identified as very low frequency (VLF). A different type of audio surveillance transmitter is manufactured which operates in this region but uses the electric power lines or telephone lines for transmission of the signals. These FM modulated

devices operate between 50 KHz and 300 KHz. At these frequencies very little radio energy is radiated into space. What these signals will do, however, is to move along almost any wire path, including regular power lines. These transmissions are known as carrier current transmissions because of this characteristic. This method of communications is used by many of the wireless intercoms sold commercially and a few audio eavesdropping transmitters.

Carrier current transmitters are usually prepackaged into electrical appliances, lamps, and wall sockets. They are not considered to be sophisticated but are modestly expensive when purchased through a "law enforcement supplier". The less expensive devices may be fabricated by repackaging a commercial wireless intercom, and shorting the OFF switch so that the circuit is perpetually on. Figure 21 illustrates the application of carrier current type devices.

Eavesdropping devices which use carrier currents offer one principal advantage over those which transmit through space. They are not normally detectable by radio receivers or other r-f sensing, debugging equipment, since they radiate little energy. A disadvantage, however, is that transmissions may be blocked by power transformers which exist regularly in an electric powerline distribution network. This feature can severely limit the range of a carrier current transmitter, and this device is only used in situations where the listening post is located within a short distance from the bugging device. To determine effective range the eavesdropper may wish to run tests, because in many power systems throughout the country, power transformers are made to pass carrier current transmissions and not block them. If this is the case, the range may be several blocks. The reason for this bypass feature is that power companies themselves use these currents for remote switching and load control. The practice of bypassing power transformers may be common for the power companies, but it is a dangerous activity for the eavesdropper to undertake, so the existence of an unauthorized bypass is most unlikely.

The use of carrier current devices on other than power lines is less common. A limited range audio system could be made to operate in a similar fashion over telephone lines, intercom lines, public address systems or security system wires.

Microwave Devices. Devices operating outside the standard radio broadcast frequency ranges tend to be more secure because the receiver needed for reception may not be readily available. A few manufacturers offer eavesdropping devices that operate at frequency ranges above 500 MHz. These units tend to be very expensive because of their complex design and difficult fabrication. The science of microwave radio signal propagation is important and significantly affects the utility of these surveillance transmitters. These high frequency radio signals have difficulty passing through many building materials, such as concrete and brick, and for this reason the transmitted signals should be directed at the receiving site over a path where there are no solid objects to block the way.

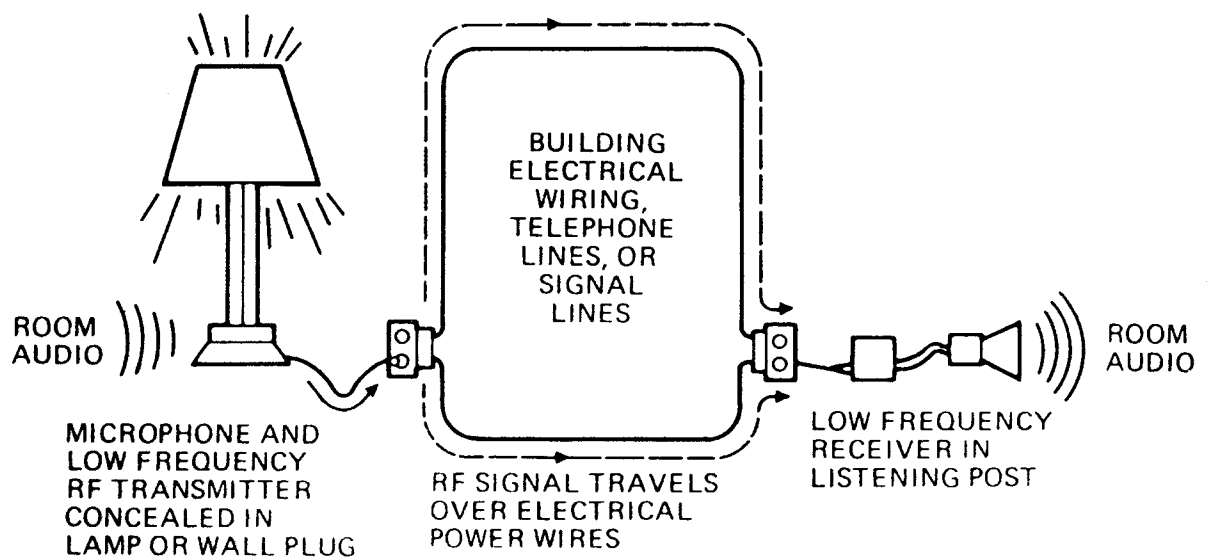
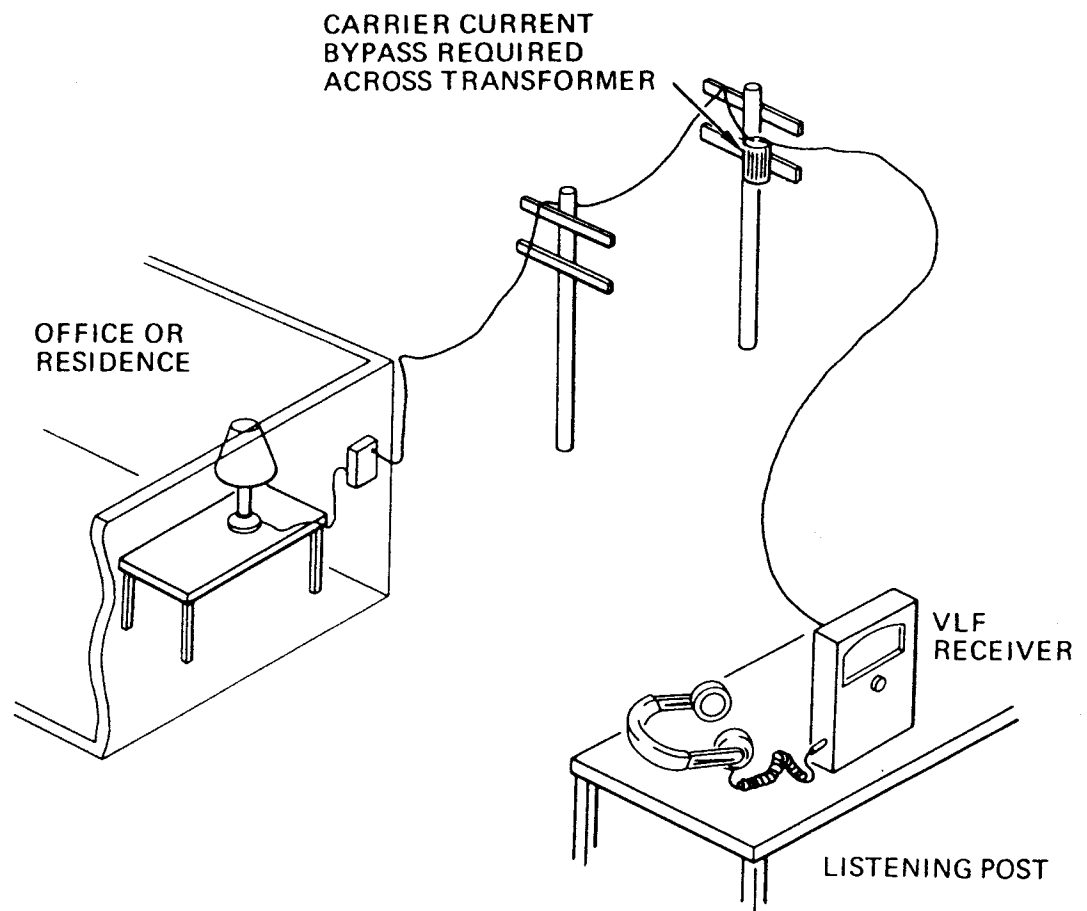


Figure 21: Carrier Current Transmitter

Passive Reflectors. This group of radio-devices will operate for an indefinite period, offer a high level of security, and require no batteries or other power source. These transmitters are strictly passive. The first publicity associated with eavesdropping devices of this nature occurred in 1952, when it was discovered that a carving of the great seal of the United States, a gift of the Russian government hanging in the American Embassy in Moscow, contained such a device. This device operated at 330 Mhz and was a small metallic capsule three quarters of an inch in diameter with a nine inch antenna capacitively coupled to it. Figure 22 illustrates such a device. The complete system includes a high powered radio transmitter which beams its signal at this reflecting capsule and a receiver to receive the reflected signals carrying the audio information. These capsule devices act as radio signal reflectors which capture and add the audio signal during the process of reflection. The devices accomplish this function by making one end of the capsule a very thin metallic diaphragm which vibrates with the room sounds. The signal is reflected from this vibrating surface and carries the modulated radio signal to the receiver for recovery of the audio.

Remote Switch Receiver. The switch receiver is a remote controlled device that can be used advantageously with any eavesdropping radio device. Sophisticated remote radio control units are sold through many electronics suppliers for a multitude of purposes including control of irrigation systems, activation of portable telephone call pagers, as well as audio eavesdropping devices. This device provides the eavesdropper with an ability to control the operating time of room monitoring equipment and achieve two distinct advantages. The eavesdropper can conserve battery power and reduce chances of detection by a sweep team by turning the transmitter on only during a time of interest.

To use the remote switch the eavesdropper attaches the device between the room bug and its batteries. Rather than physically turning the bug on, the unit is electronically activated from the remote point by turning on the control transmitter.

The Tape Recorder. The tape recorder is a basic tool of audio surveillance. Its commercial availability and the adaptability to eavesdropping makes the tape recorder one of the most widely used surreptitious audio penetration devices.

Optical Directional Systems. Surveillance systems that operate using directional beams of light energy represent another dimension in eavesdropping technology. These systems may use laser or infrared beams, but it is the laser which holds a unique position among electronic surveillance devices because of its futuristic and apparently sinister nature.

The laser has been maligned by casting it in the role of a surveillance device because of a lack of understanding of the laser-surveillance concept on the part of the general public. There are two basic types of

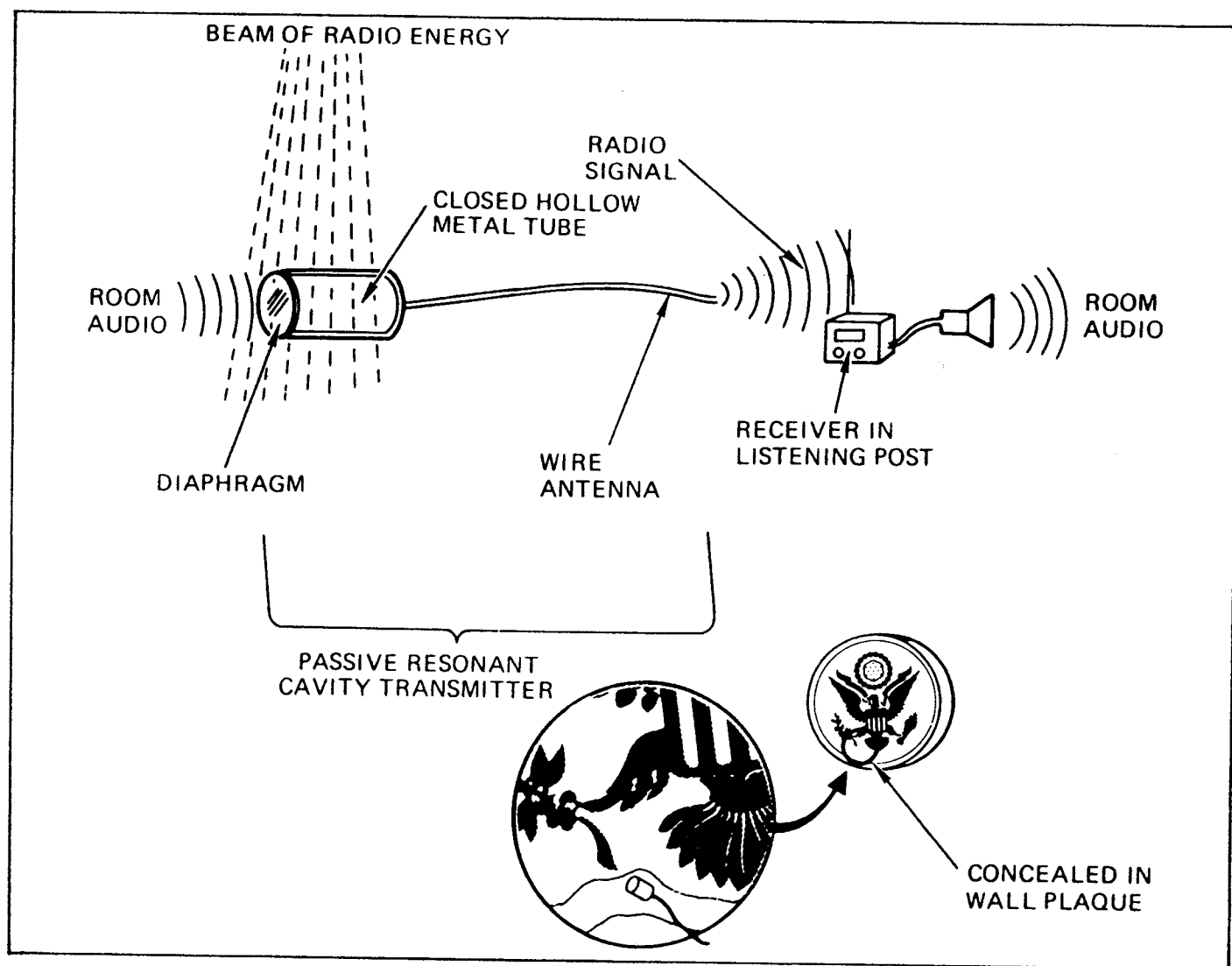


Figure 22: Passive Cavity Transmitter

light beam devices whose characteristics and applicability to the surveillance market vary widely. Small solid state devices generally called light emitting diodes (LED) can be manufactured to produce invisible infrared or visible light. These LED devices are commonly used in display of numbers in pocket calculators and electronic wrist watches. Solid state LEDs produce a fairly wide energy beam which generally spreads more rapidly with range than beams produced by lasers. The laser is much more expensive than the LED and produces a tight, coherent beam of visible or invisible energy. The beams produced by these devices can transmit greater distances and suffer a lesser degree of degradation due to beam spreading.

The device producing non-coherent energy can be used in communication transmission links instead of radio transmitters. For example, a small semiconductor LED, couple with a microphone, power supply, and modulator, could be used as a covert transmitter. When amplified, the voice modulated current or voltage produced by the microphone could modulate the light emitted by the LED. The modulated beam could then be detected by a sensitive optical device some distance from the transmitter and the audio signal retrieved. This is illustrated in figure 23. The detection of this type of device is extremely difficult, if the installation is well made and the device is protected from discovery by physical inspection or daylight background.

The solid state light beam devices which produce energy in the infrared and visual spectrum are easily obtained, as are the photo cell detectors or receivers at a listening post. Systems are produced for the commercial market which are designed for short range transmission of audio and television communications. The use of solid state optical devices is generally restricted to this type of application because of their range limitation. These systems are not particularly adaptable to clandestine eavesdropping systems.

Recently, an article in the Washington Post newspaper described the "tremendous threat" presented by the telephone company's move to use light emitting diodes in push-button telephones for illumination. It would be technically possible to modulate, with the audio in the telephone instrument, one of these light emitting diodes so that a detector in the ceiling above the telephone could capture the conversation and transmit the information to a listening post. Such an installation could be demonstrated in a laboratory. But from a practical standpoint, the complexities of detector location and telephone instrument manipulation imply that the system is operationally impractical. (A countermeasure or protective action taken by the user of the telephone would simply consist of placing the hand over the illuminated button or removing the light generating devices.)

The coherent laser, such as that available from many manufacturers as laboratory equipment, can be used to detect the minute vibrations which

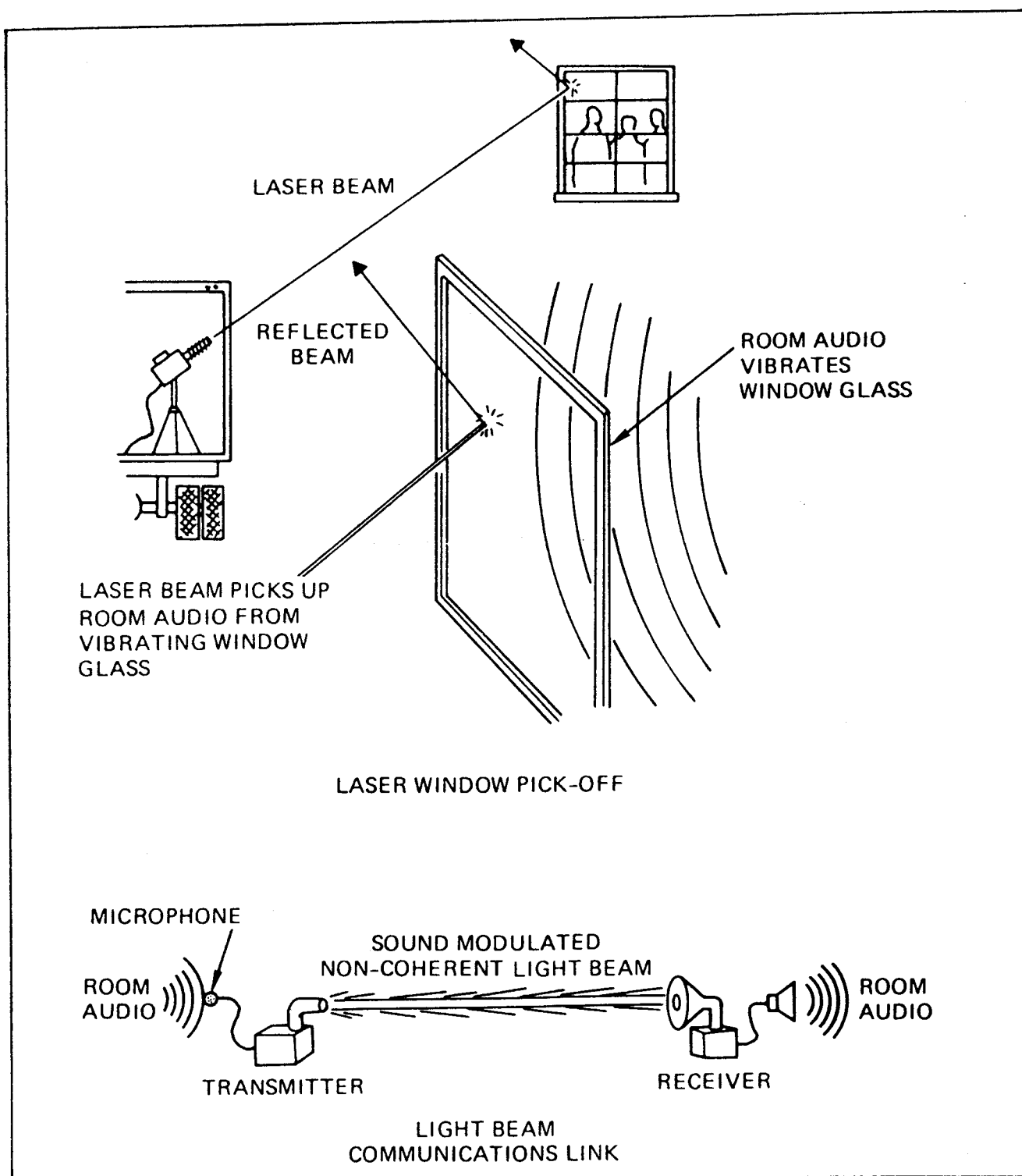


Figure 23: Optical Audio Eavesdropping.

The laser eavesdropping system, and how to make it is covered extensively in the October 1987 issue of Radio-Electronics. However, for those of you with a yen for a simpler system, it has been suggested that the following is a viable procedure:

1. Obtain any laser (infrared is best as it leaves no tell-tale trace on the observed window/curtains/wall) and a one-frequency filter which passes only the frequency of the laser light.

This is relatively expensive, but that is the bane of all laser eavesdropping systems.

2. Obtain a phototransistor sensitive to the laser light you are using, and position it so that it collects the reflected beam from your laser.

3. Couple the output of the transistor to an audio amplifier chip (#386 Tandy part # 276-1731) and the output of the chip to your headphones.

In detail the circuit is given below.

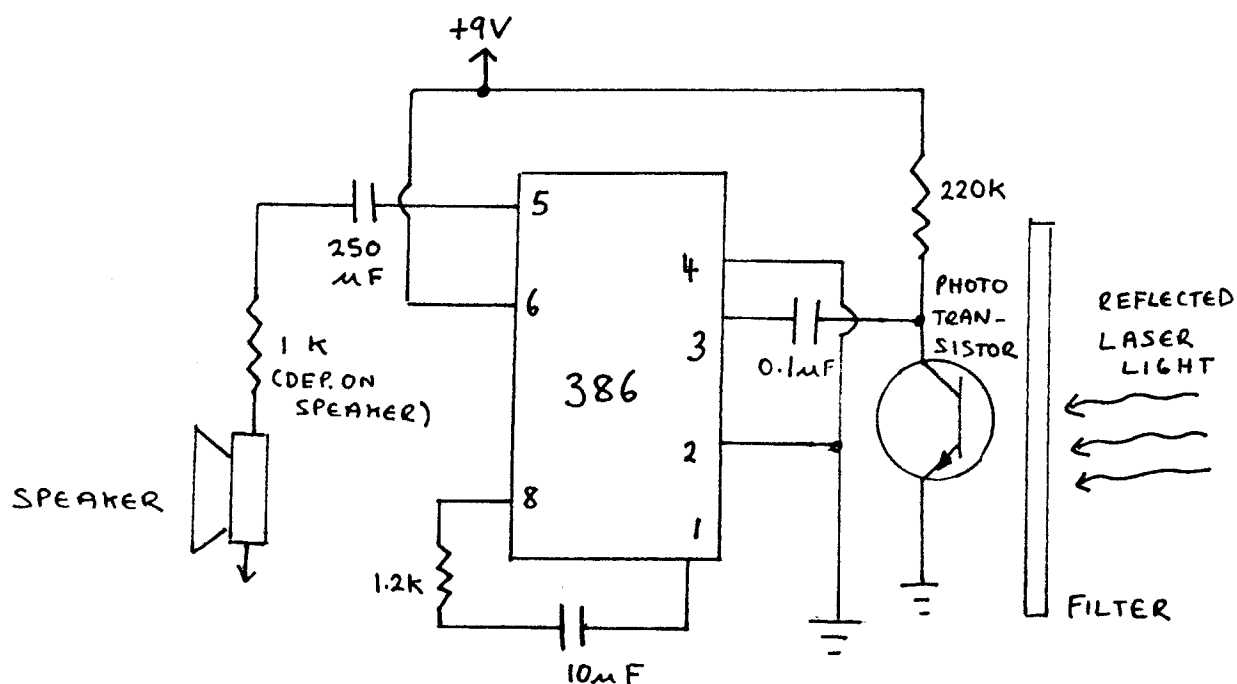


Figure 23a: Some Thoughts on The Laser Bug

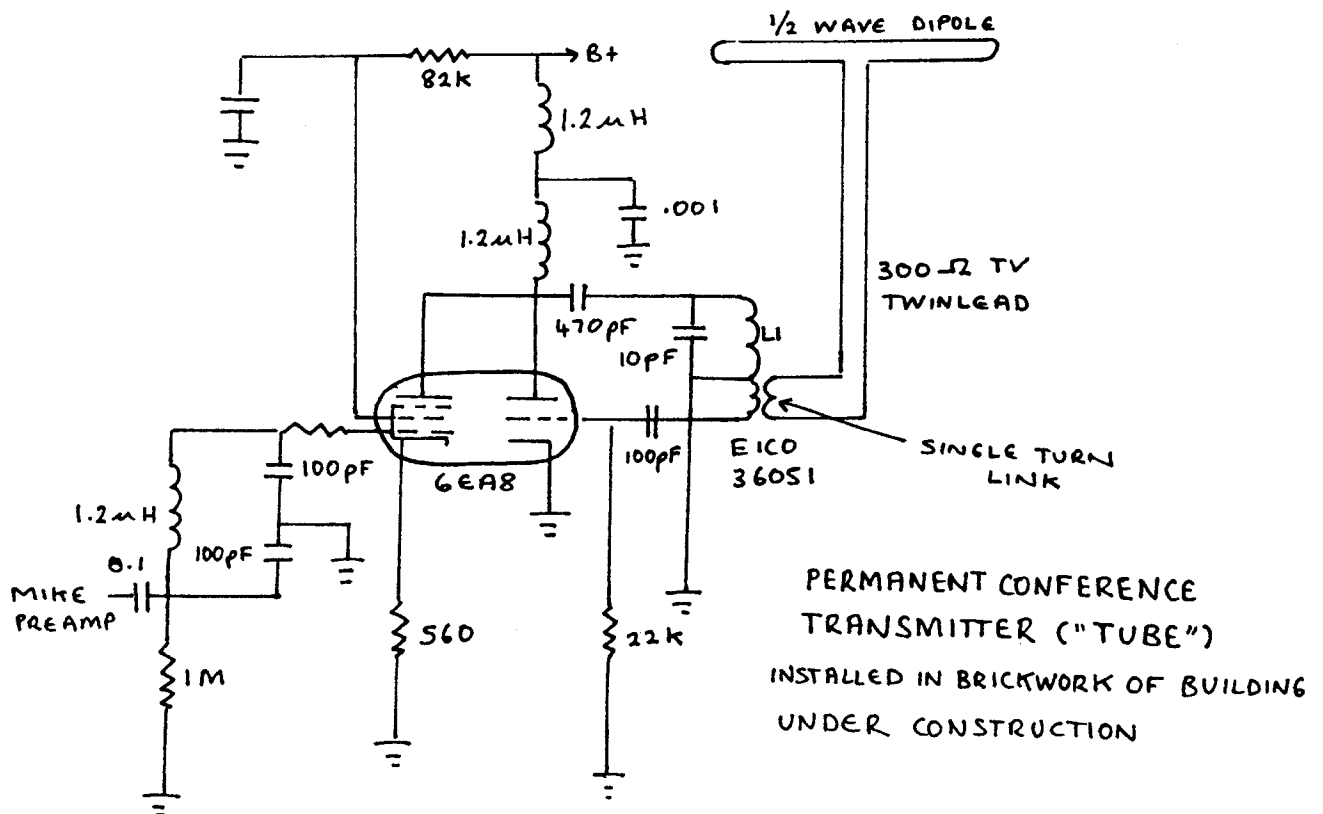
exist in a window pane as a result of nearby room conversation. The coherent laser is used because the small window vibrations cause detectable shifts in the incident beam's wave length. These shifts are then carried on the return beam back to the receiving site where they are demodulated to recover the room audio. This technique is illustrated in figure 23. Some problems exist with this laser window-bounce technique of audio surveillance which make its use difficult and expensive. Noises, such as traffic noises, building vibrations due to machinery, air conditioners, fans, running water, plumbing and wind, impart substantial vibrations onto the window surface. To retrieve small audio vibrations from the maze of signals is not a reliable or practical source of audio intelligence.

In summary, the laser is not a cost effective device. The use of solid state devices as a transmission link in surveillance activity is not impractical, since these devices are readily available and no extraordinary technical understanding is required to convert them into an operational eavesdropping system.

Other Devices

Other devices used as accessories to eavesdropping include bumper beepers and tail transmitters. Such devices do not transmit audio signals, but signals designed to enable the location of the device, and the poor unfortunate unlucky enough to be harbouring it.

These are relatively simple devices, the most difficult components to conceal being the antenna and power source.



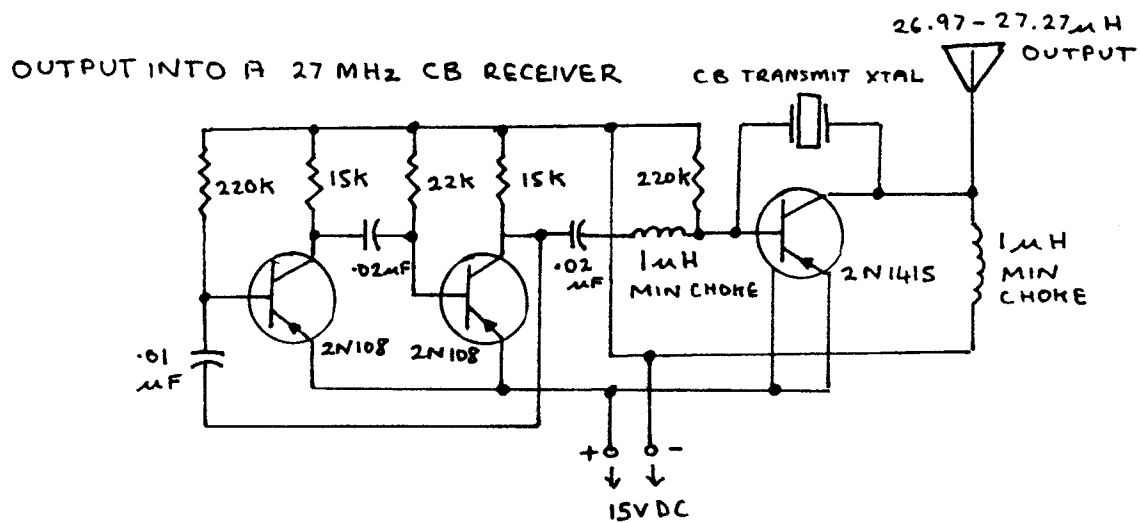
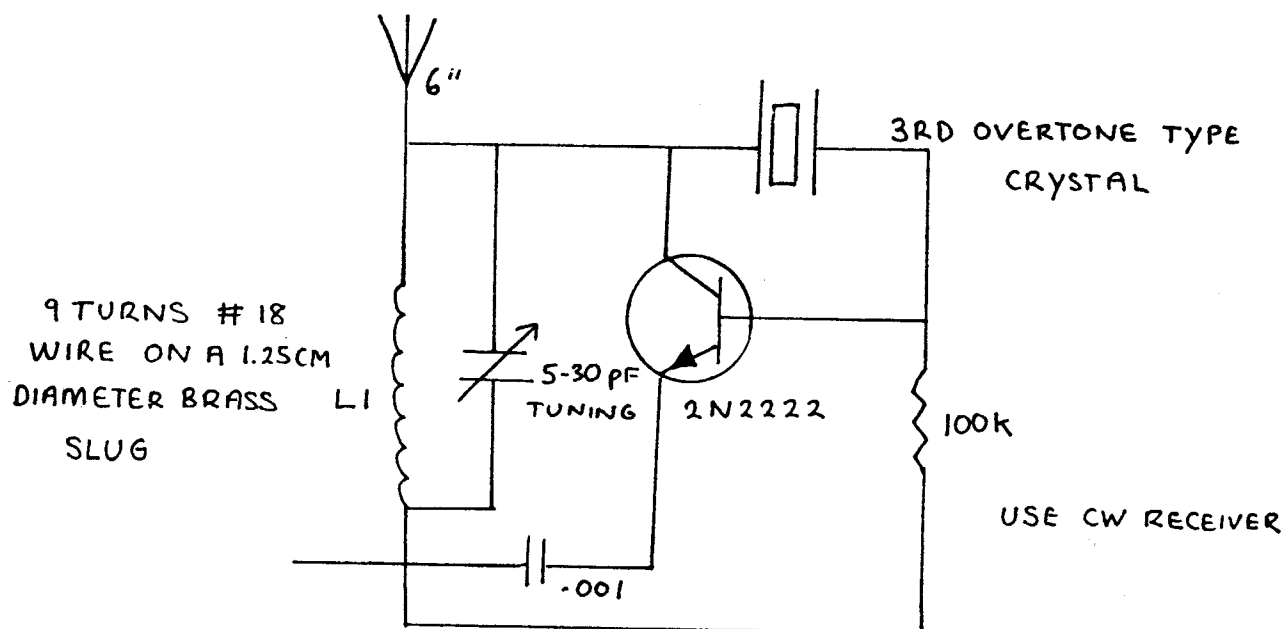
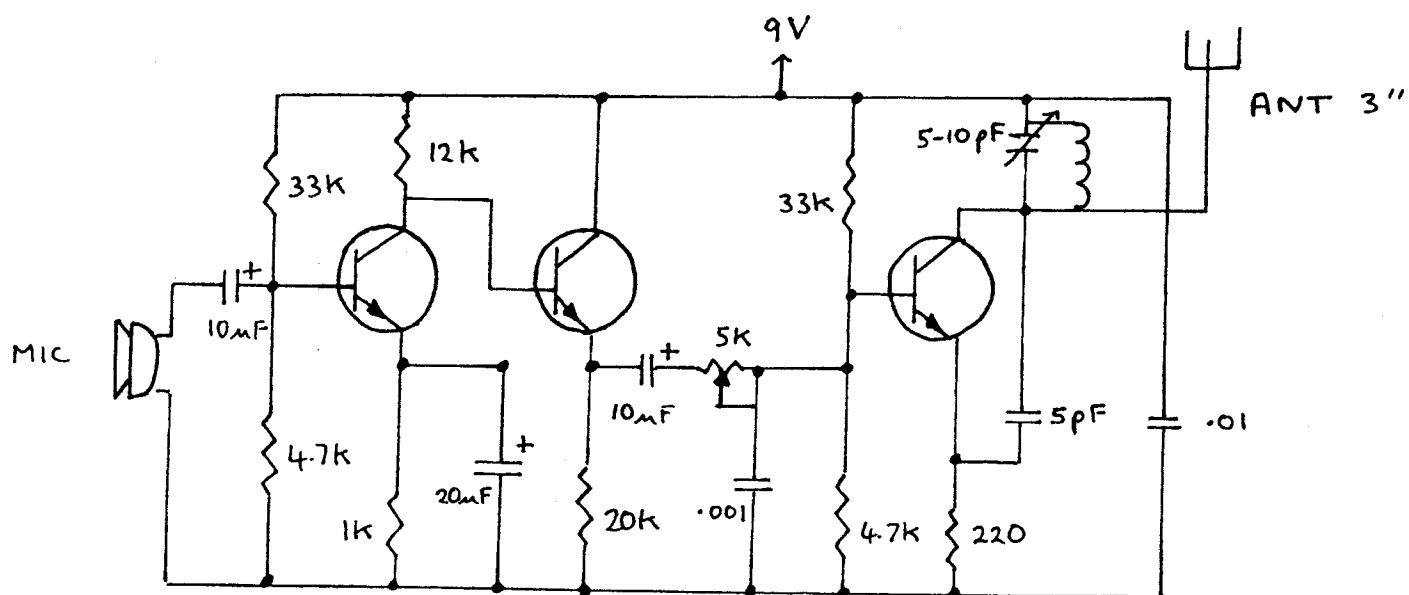


Figure 24: Tail Transmitters



L1: 6-7 TURNS #22 WIRE, 1/4" DIAM. ANY GENERAL TRANSISTORS WILL DO.

FIG 24 A: ANOTHER FM WIRELESS MIC.

L1 & L2 SHOULD BE WOUND FOR AM TRANSMISSION (SEE FIG 17). Q1 IS ANY GENERAL NPN.

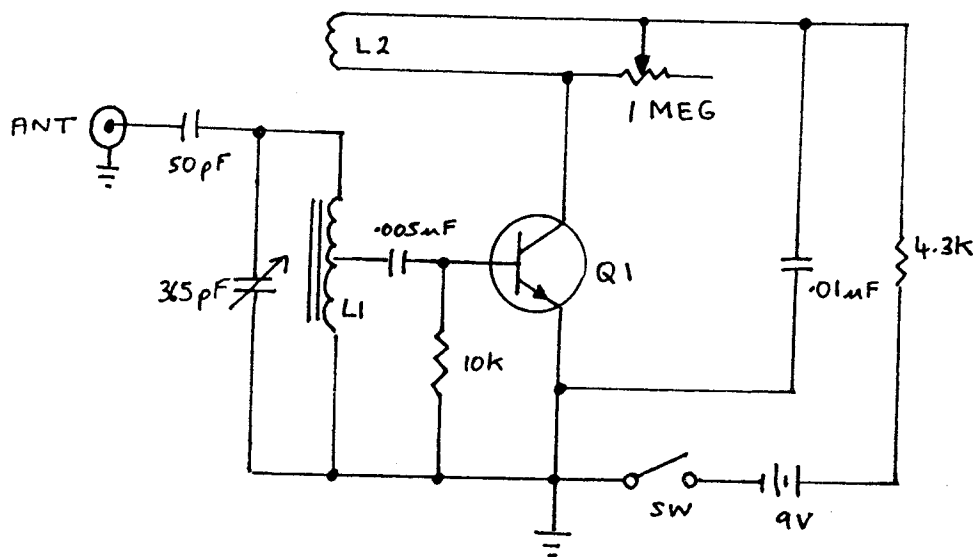


Figure 25: Bumper Beeper

Audio Security Countermeasures

Audio countermeasures (ACM), technical security measures, or simply "debugging" are terms used to describe the science of audio surveillance device detection and penetration prevention. This section examines the current status of audio countermeasures and describes the equipment available, its application, and limitations, and discusses the suitability of various devices for effective detection and protection against electronic invasions of privacy.

Telephone systems.

The telephone instrument and system are most important to the eavesdropper in that they provide numerous opportunities to gather audio information. As stated earlier, two basic types exist; those which eavesdrop on the telephone conversation and those which utilize part of the telephone system for room eavesdropping. This section addresses the security countermeasures equipment used for each threat.

Telephone taps. The telephone tap intercepts conventional telephone conversations. This section describes countermeasures equipment and procedures for each approach to telephone or conversation eavesdropping.

Wire systems. It should be emphasized at the outset that there are no existing ways to prove conclusively the existence or non-existence of a tap short of physically inspecting the phone lines. Many of the ACM devices that are currently advertised represent attempts at tap detection that in some limited circumstances could determine the presence of a tap if the tap is improperly installed or the tap is of grossly inferior quality. The detection methodology exploits the telephone system's normal switching functions by drawing current from the line when the instrument is not in use, or by simply measuring telephone line voltages. The devices which draw current from the telephone do so in such a way that, if any additional current were drawn by the attachment of a listening device or actuator switch, the total amount of current drawn would trigger the telephone company's switching exchange and cause the line to be continuously busy. Those devices which simply measure line voltage attempt to achieve the same result by detecting voltage changes caused by the attachment of listening or switch actuator devices. Neither of these methods provides any useful degree of security.

One of the problems presented in tap detection is that the target instrument may be located on the end of a very long line extending from a central station, passing through numerous cables, connected in terminal boxes, and finally entering a residence or an office. A telephone tap can be inserted anywhere between the central station and the target instrument. To check this maze of electrical wiring from the instrument end of this lengthy wire is usually more difficult than checking the system from the telephone switching station, where various currents and other line electrical characteristics can readily be measured.

Unfortunately, the individual suspecting a wiretap is not always inclined to present this problem to the telephone company for analysis. When the telephone company does check telephone line pairs from the central station or from various points between the central station to the target instrument, certain unusual characteristics can indicate the presence of a non-professional tap.

The difficulties of tap detection primarily result from the characteristics of the telephone line itself, as the electrical characteristics of any given pair of telephone wires will change with humidity, temperature, lengths of line to the central station, and equipment additions within the system. These changes can be much greater in magnitude than the changes caused by the attachment of an efficient, high quality wiretap device.

A more sophisticated system sends pulses of energy down the telephone wires; these pulses are then reflected from electrical junctions along the wire back to the source. If a wiretap is inserted, it will appear as a new electrical junction. This approach is only usable in situations where a good knowledge of the system installation is known since reflections from existing equipment would not indicate improper additions to the system. This technology is called time domain reflectometry and is too complex to be done by other than skilled personnel.

The only tap devices which are detectable are those attached to the telephone line which draw an excessive amount of current causing subsequent changes in the system voltage. Such tap devices can be detected with very simple equipment costing far less than some fraudulent tap detection systems being sold. For example, a \$20 volt meter could provide the same level of confidence in tap detection as some equipment offered for sale for nearly \$3 000. None of these ACM devices will detect the attachment of wires or voltage actuated switches which use matching networks, or which sense voltage changes between a single telephone wire and earth ground, or systems which are inductively coupled to the telephone line and are voice actuated. All of these techniques are possible telephone line surveillance practices.

There are only two recognized methods of telephone tap protection: the first requires discontinued use of the telephone instrument for the conveyance of secure information; the second is the use of quality audio scramblers. Neither protects against a tap; both are designed to protect against an interception of information. There are no scramblers available which will completely protect against a telephone tap, the only available systems merely make it more difficult for a tap to be successful. The scrambler disguises the audio signals that pass over the telephone lines by carefully mixing the signals in coded fashion at one end of the conversation and unmixing them at the other. It provides a measure of protection against hardwire and radio telephone tap systems.

Scrambler technology and prices vary widely. Pairs of scrambler devices may cost as little as \$200 to \$400 and are quite simple in their signal processing. These devices offer protection from less technically competent eavesdroppers and are perhaps effective for a short period of time against

the eavesdropper who is equipped with some technical knowledge and laboratory equipment. Expensive scramblers cost several thousand dollars and use digitising techniques, which can be quite effective. They may perform poorly over long distance lines because of limited channel band width and the time taken for the electrical signals to travel back and forth. They usually perform much better over radio communication links because propagation time is less of a factor. Currently there are no systems available which offer absolute security over conventional telephone lines, and only the special wide band systems used by government agencies are considered secure.

Radio Systems. Electronic detection of a telephone tap transmitter installed on the target premises is much the same as detection of any other radio transmitter eavesdropping device. The only difference in the devices is that the audio signal is supplied by the telephone line instead of room conversation. The radio tap devices, however, have one major advantage over room transmitters in that they need not be installed near the premises where the target instrument is located and may be attached to the telephone line at any accessible point. Therefore, chances of discovery by either physical search or radio spectrum search may be limited. Location of the installation is the principal difference between effectively detecting a radio telephone tap and a radio room bug by the means described earlier. Several characteristics should be mentioned, however, which make radio telephone tap detection unique.

Since the telephone tap transmitter is designed exclusively for the interception of the telephone conversation, as a general rule the telephone must be in use before any radio spectrum analysis can begin. This is achieved by placing the instrument in operation by calling a cooperative telephone and conversing in a non-alerting manner. The telephone transmitter should be activated by this process unless a remote switch receiver is being used and is deactivated at this time. If this is the case, only physical inspection will discover the tap. It should be noted that an r-f search will not be effective unless the device is within the operating range of the detecting device.

There are few practices which can protect against r-f telephone tap devices. The only device offered on the commercial market is an r-f jammer, which is illegal in most states (see figure 30). Another method is the employment of shielded rooms, provided that the transmitter is located within the shielded area. This is discussed later.

One manufacturer claims that if a device were connected to the telephone line pair at the target telephone that could raise and lower the telephone line voltage at a slow rate, perhaps four or five times a second, radio eavesdropping devices that use the telephone lines for power would be upset and possibly suffer a momentary frequency change in their transmission. In the listening post this sudden change of frequency would cause momentary loss of audio in the eavesdropper's receiver.

Telephone Room Eavesdropping Devices

Each of the telephone system eavesdropping devices discussed earlier may be detected through the use of various electronic technologies or their effectiveness reduced by use of specific electronic protective devices or procedures. The following sections address these countermeasures devices and procedures.

Infinity Transmitters, Listen-backs and Keep-Alives. The detection of an active infinity transmitter is relatively easy, but the intentional activation of a quiescent device by a sweep team is not easy. Several manufacturers offer countermeasures systems which are designed for direct attachment to the suspect telephone lines. These systems emit variable frequency tones which sweep the audio spectrum in an attempt to trigger the implanted surveillance device. In newer infinity devices available on the European market, the simultaneous presence of different tones, or time-spaced tones is required to activate the transmitter. The currently available tone activation counter-measures devices do not affect these multiple tone units; however, a few manufacturers, aware of the multi-tone requirement, may soon produce multiple tone sweeping units. Though tone sweeping is designed to trigger the infinity device, actual detection is accomplished by determining that the device has responded by electronically picking up the telephone. For example, the tone sweeping generator is connected directly to the telephone wires through a matching network, and the telephone instrument is left on-hook causing the line voltages to remain at the normal 48 volt level. Then, if the generator produces the proper triggering tone or tones and activates the infinity transmitter, the line voltage drops to between 6 and 12 volts, a change which is easily measured with a conventional voltmeter. As an alternative, if the target phone is dialled from a remote location and the proper tones are placed on the line through the mouthpiece of the instrument, the telephone at the target will stop ringing and room audio will be heard. If the telephone continues to ring, the infinity device is either not present or has not been activated. Equipment that places audio tones on a telephone line is available for \$130 to \$150. The more costly telephone instrument inspection systems frequently contain audio tone generators in addition to the equipment required for complete instrument analysis. Other inexpensive devices are available which monitor voltage levels only. These connect directly across the suspect telephone lines and do not activate the infinity device. They merely monitor the voltage level on the line and, should an infinity device be activated while the telephone is in the on-hook position, the change in line voltage is immediately detected. These devices are especially applicable for use on single line telephones where there is no lighted push-button to indicate telephone line use. They are usually priced between \$90 and \$130 and require installation over long periods of time to increase the probability of detection, and should be used continuously to attain a high level of confidence.

The detection of listen-backs and keep-alive devices requires either

telephone line voltage monitoring or audio detection equipment. When the eavesdropper dials the target telephone from a remote location and the target instrument is answered and then hung up, the keep-alive device keeps the telephone line open, permitting the eavesdropper to overhear room audio. Tones do not activate this device, but it can easily be detected by calling the target telephone and duplicating this procedure. The line voltage monitor unit already described can indicate that a listen-back device is in use since the line voltage generally remains below 12 volts after the instrument is hung up when it should be approximately 48 volts.

On-Line Microphones. As described in an earlier section, microphone devices which monitor room conversations can use telephone lines for short range transmission of the audio from the target area to the listening post. They may be electronically detected, while operating, only through the use of an audio amplifier connected across the telephone lines being used. However, because audio signals may be transmitted over any suitable pair of wires, detecting these devices becomes more difficult in the case of the multiline instruments with their fifty line cables. Considering the redundant wires, ground wires and signal wires, there are 1225 possible line pairs available to pass audio. To monitor all of these combinations is cumbersome and inconclusive. If the on-line microphone incorporates some voltage switch activating technique, room audio would not necessarily be present at any given time, nor would the switching element be easily stimulated, because of the vast number of possible activation signals. No manufacturers are known to supply telephone line voltage stimulation equipment designed to activate devices of this nature because of the potential damage they might cause to the telephone system itself as a result of the various applied voltages.

Telephone Modification. The basic electronic tool used to check for telephone modifications is the telephone modifications analyser or checker. This piece of equipment allows the operator to select two individual wires in any combination from a large number of wires in the 4 to 50 wire bundles which extend from the base of the standard telephone. The operator generally disconnects the cable at a convenient junction point, usually at the wall connector block, and attaches the end extending from the instrument to the analysis equipment, leaving the other cable end free and unconnected. After the attachment is made to the telephone analyser, the operator systematically selects each possible pair combination and tests the pair to determine its electrical characteristics. In the case of the 50 wire cable, there are 1225 practical combinations to check. If an internal electronic modification exists, the characteristics of the specific altered line pair should become immediately apparent. In order to activate a device which needs some form of electrical stimulation to operate, most telephopne analysers usually contain tone generators, and audio amplifiers. These tests of the instrument are to detect internal modifications only and have nothing to

do with locating a tap unless a radio tap device has been installed across the talk pair in the instrument.

Some of these devices are automated, and may be coupled with other testing devices (such as those referred to in the last section).

The protection systems offered to the public which are designed to offset the threat of telephone modification or compromise fall into two categories. One system physically disconnects the telephone instrument from the outgoing wires and thereby prevents the passage of audio from the instrument onto the wires; a second system injects a jamming signal into the instrument which masks audio by burying it deep in noise. In this latter concept the noise itself does not go onto the telephone wires, but is contained within the instrument and it is equally effective on single-line and multi-line instruments.

The basic telephone disconnect system is the plug-and-jack type found in residential telephones. This is simply a plug on the end of a single line instrument cable which is plugged into a receptacle when the telephone is in use and is disconnected when the instrument is not in use. The only requirement for use of this system is installation of an external ringer to signal an incoming call. These disconnect systems have been found to be inadequate because the user is frequently not inclined to plug and unplug the instrument each time the telephone is used.

Basically, the isolation from the telephone instrument from the wires exiting a room prevents the use of many telephone modification techniques of room audio intercept. Telephone line disconnects do not, however, protect against self-powered transmitters installed in the telephone instrument. More sophisticated instrument isolators use fibre optics to pass standard audio signals and restrict the passage of unauthorized signals to the outside wires. The cost of these devices is prohibitive, but they are available.

There are some operational techniques which can be used by the security conscious individual to inhibit successful telephone modification penetration. The first applies to the standard five button or multiline office instrument. If all the buttons are returned to the up position while the up position when the instrument is not in use, the threat of compromise is reduced because one half of the internal electrical connections necessary for the eavesdropper to perform the eavesdropping cease to exist. This occurs because the telephone instrument's internal design causes a portion of the hook-switch to be connected when one button is depressed. Left in this position, the eavesdropper must only complete the remaining hook-switch bypass to accomplish an operational compromise.

Radio Eavesdropping Detection

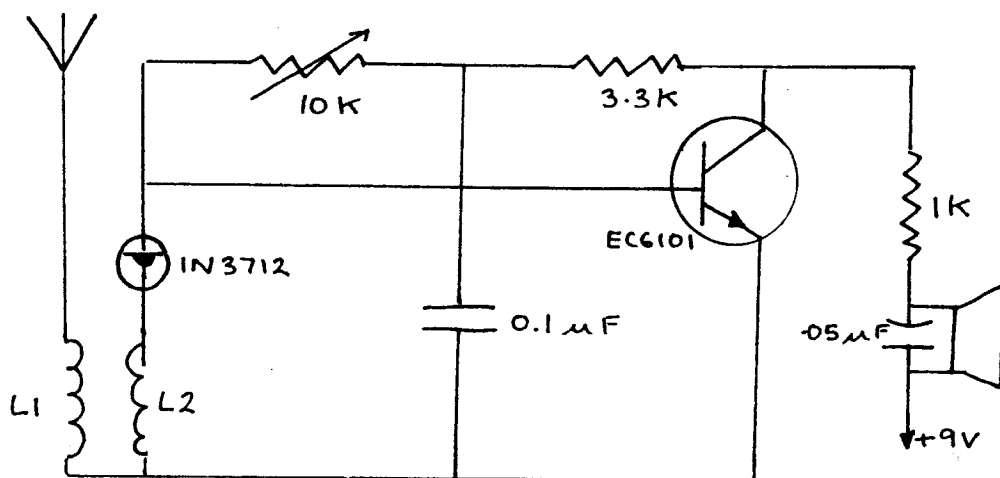
The detection of radio transmitter devices requires the use of fairly sophisticated electronic countermeasures equipment. This section provides a brief overview of the devices available to the public which afford this capability in varying degrees.

Field Strength Measurement. The field strength meter (see figures 26 and 27) is a device designed to measure the relative radio frequency energy which is present at some point in space. This broad band device indicates the cumulative total of the power present from all sources throughout a major portion of the radio spectrum. The field strength measuring device contains an antenna, a diode detector, and a sensitive amplifier which drives a meter or other circuitry to provide an indication of the relative r-f energy intensity detected. This measurement is usually displayed on a meter but may also be represented by an audio response or a simple indicator light. Fabrication of a field strength meter by an individual is possible for an investment of less than \$50 in parts.

The basic field strength measurement device has been refined and made sophisticated. In some cases controls are added to allow the operator to normalize or null the meter to the local environment as in a region of high r-f background energy, such as in the middle of a city. This concentrated energy would saturate the detector and indicate a continuous "active" condition. Other refinements include the addition of a limited tuning capability in which one wide band is broken into small segments to permit discrete amplification of the energy within a particular frequency segment. Frequently, the output of the field strength meter is amplified to a high level to operate a speaker contained within the unit. If the device is placed in the vicinity of an operating radio transmitter microphone which is using AM or FM modulation and the transmitter is of sufficient power, there is potential for creating a feedback "squeal" between the transmitter and the speaker in the field strength unit. This detection method, although not necessarily conclusive, could be highly alerting to a potential eavesdropper and is generally not good practice if further efforts are planned to locate the listening post as well as the device.

An alternate of this feature requires the field strength meter output to be demodulated so that the operator can monitor the audio of the transmitted signal in a non-alerting manner to determine the presence of a clandestine transmitter. As field strength measurement have become more sophisticated, single packages are available that contain two field strength measurement circuits and use dual antennae operating in a differential mode. The principle of operation used in this device takes into consideration antennae placement and differential energy measurement. One antenna, being closer to the surveillance transmitter than the other, will receive a different amount of energy than is detected from the other antenna. The difference in energy or signal strength at each antenna is closer to an operating transmitter than the other. This tends to reduce the effects of distant, high-power, commercial transmitters, since the field strength appearing at both antennae would appear essentially the same.

All of the field strength measurement "debugging devices" reviewed during the study are combinations of the foregoing options, each option providing somewhat different capabilities. All devices suffer the basic disadvantages of broad band diode detection (see fig 28). The diode



L1: 6 TURNS #18 WIRE ON A 1-1/4 CM CORE. L2: 8 TURNS

Figure 26: Field Strength Meter.

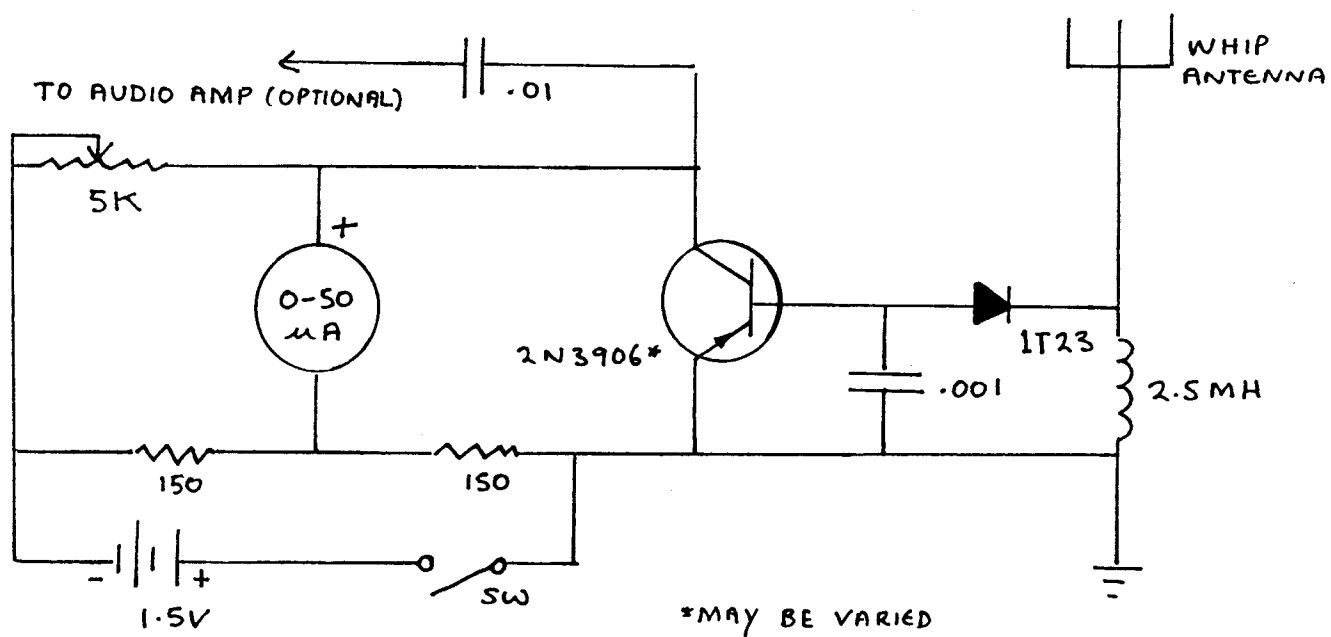


Figure 27: "Bug Detector"

detector, field strength meter, or crystal detector, all synonyms for the same device, has limited application in the practice of countermeasures inspections. It should not be relied upon as the principal means of radio transmitter detection. These devices are relatively inexpensive, costing from \$20 to \$300 depending on the options offered and the quality of manufacture. Limitations of these devices include broad spectrum width with corresponding large variations in sensitivity, poor selectivity, inability to detect carrier current devices, and susceptibility to standing wave reflections which occur inside buildings.

The field strength measurement device is usually unable to detect low power eavesdropping devices which are transmitting in high r-f backgrounds or devices operating near the frequencies of large, high-powered commercial broadcast transmitters. This inability to locate r-f transmitters in high noise background environments significantly reduces effectiveness. The field strength meter, however, does have a place in countermeasures as a secondary or back-up probe in r-f detection.

Countermeasures receivers. The major and important difference between countermeasures receivers and those receivers commonly used for commercial broadcast reception is that the countermeasures device is designed to search a large portion of the r-f spectrum, isolate and identify a signal, and demodulate the signal to ascertain its nature and information content. It is often erroneously assumed that clandestine radio transmitters operate between 88 Hz and 108 MHz, the commercial FM broadcast band. Instead, it should be assumed that the entire spectrum is available to the eavesdropper and can be used with the application of available technology.

Requisite technical characteristics of surveillance or countermeasures receivers demonstrate high sensitivity and selectivity over the large radio spectrum, are capable of many different demodulation techniques, exhibit frequency stability and capability to acquire weak signals, and demonstrate high rejection of unwanted signals in adjacent frequency ranges. None of these capabilities is normally provided in receivers other than counter surveillance receivers. The frequency range of the receivers should at least cover the operating range of presently available transistors whose price allows them to be used for fabrication of surveillance transmitters. Frequently an FM broadcast receiver is used as a countermeasures receiver, but it is limited not only in frequency range but also in ability to detect low level signals and sub-carrier signals which require a greater band width and additional demodulation capabilities. As shown in figure 28, the commercial receiver band width is not wide enough to allow reception of sub-carrier transmissions. This illustration is a visual display that may be added to the countermeasures receiver and is called a "pan adaptor". It provides a picture of many radio transmitters' signals and their relative strength in the portion of the radio spectrum being analysed.

Usually the automatic frequency control (AFC) of commercial FM receivers prevents them from being tuned to lower power signals such as those transmitted by a surveillance transmitter because the receiver will

automatically lock on any adjacent signal from a high power commercial broadcast station. (Recall the practice of snuggling or of placing a low-power, clandestine transmission adjacent to a high power broadcast signal.) One other drawback to the use of commercial FM receivers regards that inherent inability to cover their own intermediate frequency (IF), usually 10.7 MHz. The design of these receivers precludes their operation near these frequencies and the skilled eavesdropper can fabricate devices that operate near this frequency range. Likewise, the wireless microphone designed to operate in the FM region can be tuned outside this frequency band.

The quality countermeasures receiver may be manually tuned or computer controlled for automatic cycling through the spectrum. Systems of this nature are available on the commercial market, but their prices range from \$50 000 to over \$100 000, depending on the characteristics desired, such as frequency ranges involved, types of modulation, and extent of automatic processing.

A few manufacturers produce quality portable equipment. These receivers are quite popular and cost between \$6 000 and \$11 000. They generally satisfy the requirements of providing broad frequency coverage and various demodulation techniques, including FM, AM, upper and lower single side band, and narrow band FM. In addition, band widths are frequently adjustable from 1 MHz to 10 MHz. Better quality units will provide a signal display capacity on a pan adaptor. This last feature is considered a necessity since it provides the operator with the ability to assess visually the sophisticated modulation techniques, the presence of subcarriers and snuggle devices, and improves the general flexibility and usefulness of the entire system. These surveillance receivers are fully capable of locating and identifying any of the transmitters described in the first chapter of this book with the exception of those which cannot be detected due to a specific frequency being used that is beyond the range of the receiver or because remotely activated transmitters are in the "off" mode.

The only unconventional modulation technique used in radio surveillance devices which are commercially available is the sub-carrier technique described earlier. These subcarrier transmitter signals are not detectable by conventional radio receivers; they are not easily demodulated. They may be visually detected, however, with a spectrum analyser or countermeasures receiver with a panoramic display attachment. In the latter case, the receiver intercepts and visually displays the energy of the device on a small video screen, though it is not possible to retrieve the original audio signal without additional processing. As described elsewhere, two receiver detection processes are required to reproduce the desired audio. The first receiver detects the principal high frequency signal. In the next step, a second receiver processes the low frequency subcarrier signal to reproduce the original audio. To systematically test each suspect radio signal for subcarrier modulation during a countermeasures radio spectrum analysis, this same dual detection process must be completed. It is obvious that this activity can be extremely expensive and time consuming

where a large number of radio signals is involved. For this reason some manufacturers offer crude subcarrier detectors in small, easy to use packages which are designed for use with another primary receiving device. These subcarrier detectors, however, lack signal selectivity and sensitivity and, therefore, may easily overlook the lower powered clandestine subcarrier device.

If the principal frequency of a sub-carrier transmitter is received on a single conventional receiver and no provisions are made for the second processing step, the audio output of the receiver will appear muted or silent because the subcarrier signal frequency is far above the audio detection range. To gain added security, the eavesdropper may then select a major operating frequency which is exactly the same as a commercial broadcast station. This won't affect the performance of the subcarrier transmitter because the subcarrier signal is far outside the detection band width of the receiver; however, now rather than a muted audio output being produced at the receiver's speaker, the normal audio carried by the commercial broadcast station will be heard. In this manner, the basic characteristics of the sub-carrier transmitter can be used to significantly increase its secrecy since even the existence of the main carrier can be concealed.

One possible future threat regards the use of clandestine video and data services which transmit other than oral data. Not only are these devices not restricted by current laws, but their detection and demodulation can be extremely difficult without appropriate knowledge of the signal and the use of costly analysis equipment.

The surveillance receiver is a tool which must be utilized with skill equal to that of the eavesdropper. The counter surveillance expert must apply this tool in situations to detect devices that are most attractive to the opponent. For example, sweeping with receivers has no effect on the remotely switched devices which transmit data at a different time than during the sweeping. Likewise, sweeping cannot detect passive devices unless they are active during the time of the inspection. These devices must be found either through physical search or X-ray analysis. The detection of microwave links is also impossible without the use of special antennae placed in a position to receive the transmitted energy. An additional consideration often overlooked by users of surveillance receivers is that of the normal receiver whip antenna. The single fixed length antenna commonly used over the 30 MHz to 1000 MHz frequency range will show repeated and predictable nulls in its ability to receive specific frequencies. This effect is caused by the fixed geometric relationship between the physical length of the antenna and the wave length of a specific radio frequency. If this relationship is improper, the energy level of the specific frequency being received will be reduced, thereby making it possible for the radio receiver to overlook the signal because of its apparently small signal strength. Suitable antenna systems which can overcome much of this lack of performance are available at prices up to \$2000. However, one skilled in the art of countermeasures can

manipulate antenna lengths and the placement of receivers during the sweep to overcome many of these deficiencies.

Another use of the low frequency counter surveillance receiver is in the detection of VLF carrier current transmitters. Detection of VLF transmitters is generally not possible by anything but a VLF receiver which should have good sensitivity to detect the low power signals, and exhibit good selectivity. (These receivers are also used in the second demodulation process for the detection of sub-carrier signals.) This level of performance cannot be achieved with the less expensive devices offered by commercial product manufacturers. Those offered for sale can only detect higher powered, carrier current devices within limited ranges. These counter surveillance VLF receivers are connected directly to the power lines or telephone lines with special voltage isolation adaptors to prevent high voltages from damaging the receiver or injuring the operator. The low frequency spectrum is scanned in much the same fashion as with the higher frequency countermeasures receivers. It should be re-emphasized that the carrier current transmitter radiates very little r-f energy into space and is therefore not detectable without a direct connection to the lines being examined. The range of transmitters utilizing this technique is frequently underestimated. One manufacturer experimented with carrier current devices and was able to retrieve an audio signal three blocks from the site of signal initiation after circumventing two power line transformers, commonly claimed to filter and prevent transmissions of this sort. In this case, the transformers were provided with bypasses by the power company to enable it to use carrier current controlled equipment.

Spectrum Analysis. In recent years the spectrum analyser has gained an accepted place in the countermeasures electronic field due to its flexibility and capabilities for display of sophisticated modulation processes. Typically, the analyser exhibits less sensitivity than the countermeasures receiver; however, this disadvantage in some instances is offset by the ability to display a large portion of the radio spectrum and the corresponding side bands that may contain audio signal information. Newer spectrum analysers have provisions for varying the band width and displaying the spectrum to allow uncluttered reception of transmissions. Until recently, spectrum analysers tended to be large and unwieldy. In the last few years small, portable units have been developed and now are available to the countermeasures technician. Properly used, the spectrum analyser can be used for analysis of signals throughout the radio spectrum and with additional attachments can be used to analyse audio signals and carrier current signals in a manner that is not possible with a countermeasures receiver or audio amplifier.

The spectrum analyser does have certain limitations. Its reduced sensitivity requires that it be in proximity to the surveillance device for detection. Also, once a device is detected, most spectrum analysers do not provide a demodulated output. The cost of these devices is relatively high, running from \$3 000 to \$7 000 depending on the included accessories, frequency ranges, and portability. Professional organisations use the

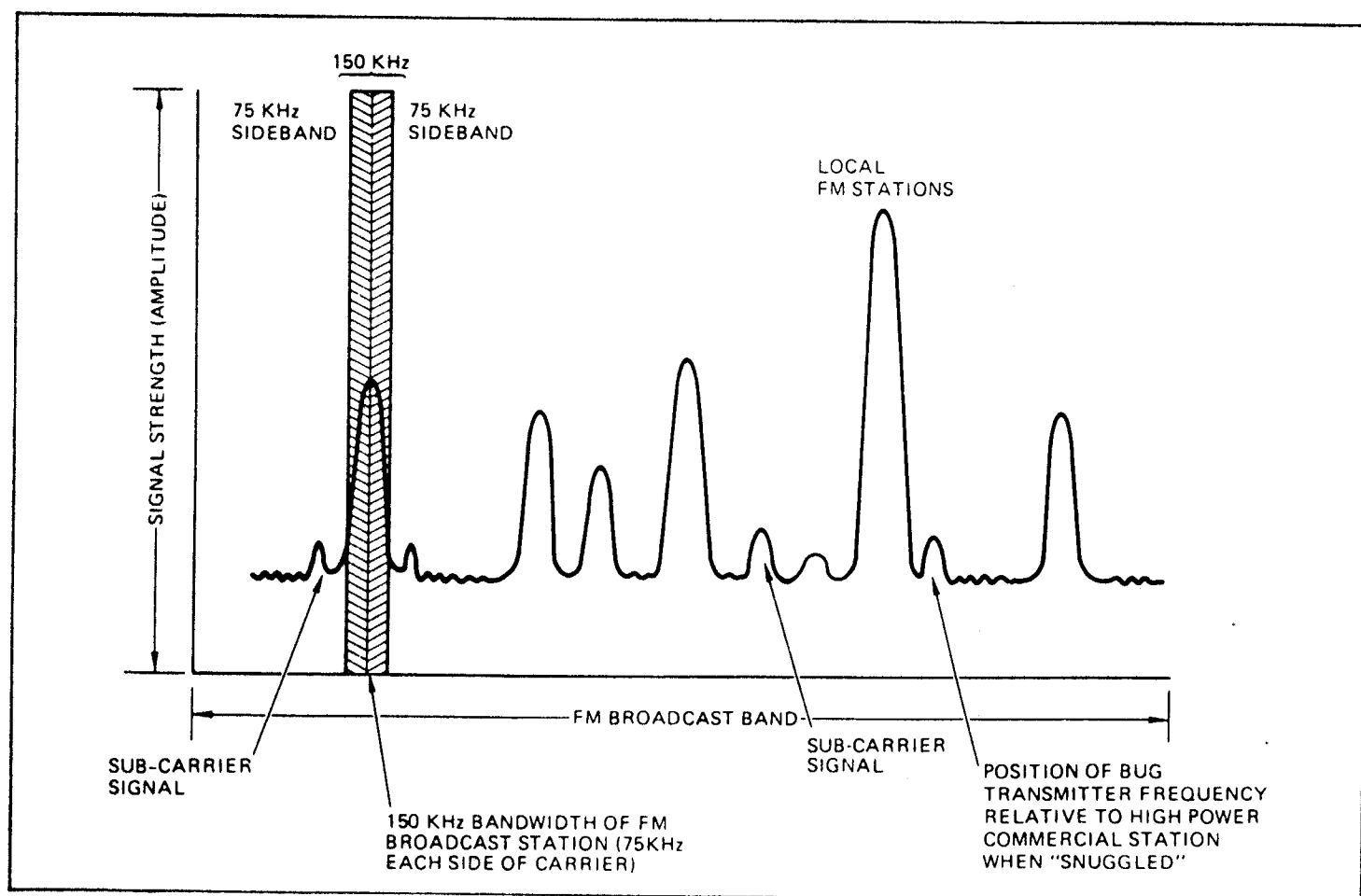


Figure 28: FM Broadcast Band Spectrum

analyser to augment the surveillance receiver, to identify those signals not detectable by the receiver, and to provide assistance in analysis through visual presentation. Figure 29 illustrates the ability of the spectrum analyser to display larger segments of the radio spectrum than the radio receiver.

Other Inspection Equipment. This section offers a brief description of other detection systems that are available to the countermeasures expert and represent additions to a basic equipment list. All of the technologies employed by these devices have been demonstrated commercially and provide increasing thoroughness to the countermeasures detection process.

For example, portable X-rays have been used for years. These units utilize either direct visual display on fluorescent screens or photography. X-ray analysis of most objects provides conclusive proof of product integrity. Complex pictures of radios, telephones and other electronic devices, however, require detailed study by experts. X-ray systems are available that weigh twenty to forty pounds and cost between \$1000 and \$3000.

The detection of optical links, including infrared and laser systems, requires the use of photo detectors. Systems of this type designed specifically for the detection of clandestine optical links are not available.

Metal detectors fall in the same category as field strength measurement devices but are used by the countermeasures expert who limits their use to inspection of completely non-metallic objects such as wooden furniture, foam cushions, or ceramic ashtrays. They have little value when used on walls, floors, ceilings and other structural members, as those areas are likely to contain nails, reinforcing bars, pieces of wire, metallic trash, and plumbing.

General Purpose Audio Surveillance Protection Systems

Acoustic protection. The basic acoustic protection system is a specially designed room within a room. Sensitive meetings may be held within this structure, and participants can be relatively confident of conversation security.

A common fallacy is that audio noise generation, such as a background radio playing in the room where sensitive conversations are held, provides good audio security by covering the conversation. This practice provides only a modest level of security, however, since this noise tends to be musical in nature and some of it can be filtered from conversation recordings because of its different frequency characteristics. Further ineffectiveness is caused by reducing the volume of the radio to the level which can only be considered background noise; if the radio volume is increased, the conversationalists merely increase the volume of their communication as well, thereby defeating the purpose of the whole arrangement. One improvement is the use of noise sources that contain audio energy distributed evenly throughout the range used by human speech.

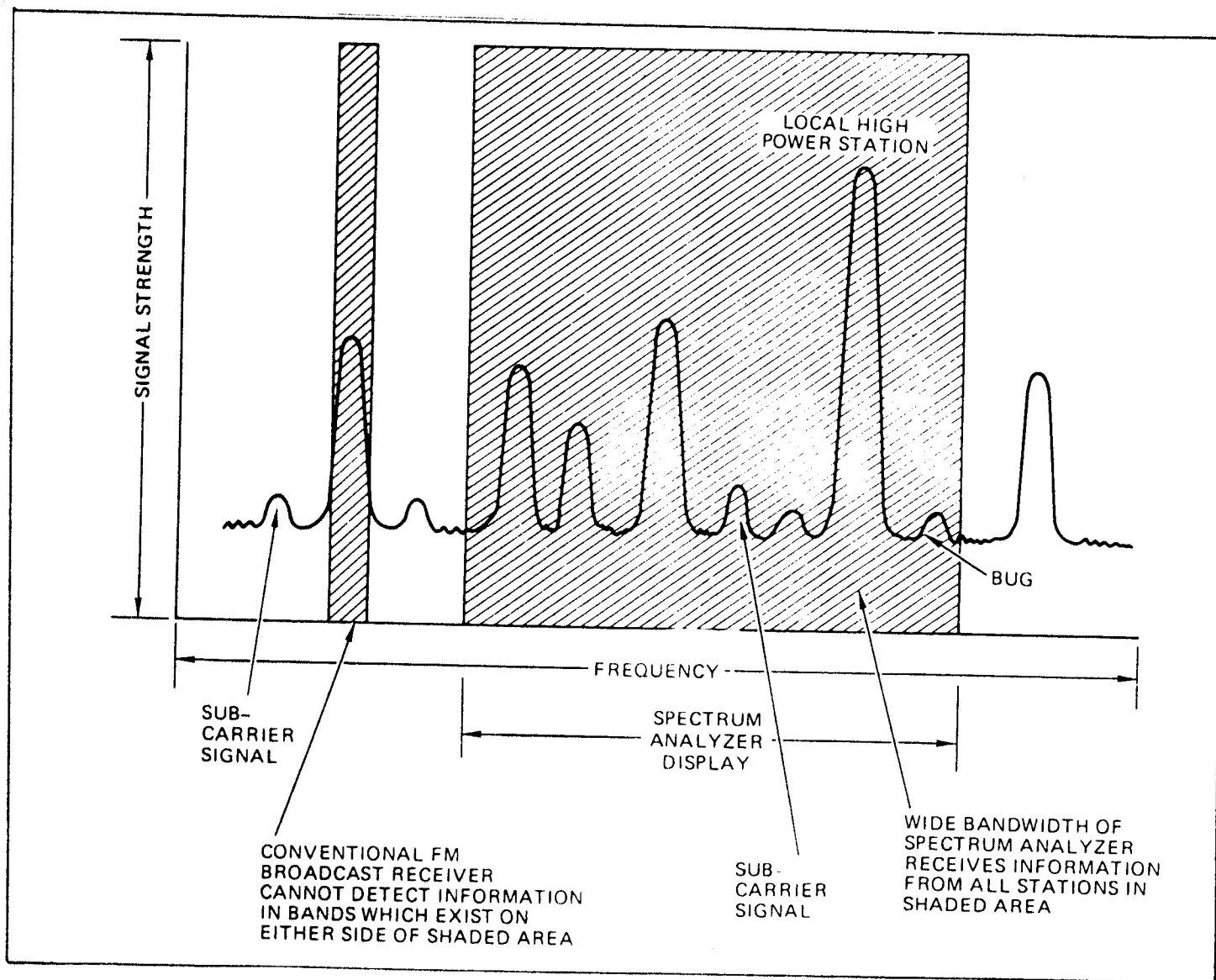


Figure 29 Radio Spectrum Display

These audio sources include running water, flushing toilets, gurgling fish tanks, window fans and phonograph records. Sounds of this nature provide the type of masking that can significantly reduce the interpretability of an intercepted conversation. The use of these technologies is widely known. However, misunderstanding of noise effectiveness as a countermeasures technique is quite apparent to laypersons. Devices which provide this masking are available commercially from a limited number of suppliers at nominal cost.

Radio Frequency Protection Systems. Rooms similar to those described in the previous section exist that protect against radio transmissions. These rooms are commonly known as r-f shielded rooms or screen rooms and are used extensively by electronics firms to provide r-f free environments for laboratory tests and analyses.

Commonly known r-f protection devices are the hash generators or radio frequency jammers which have existed since the Model-T spark coil. The r-f generator supposedly renders a radio surveillance device ineffective by generating a high level of random noise or static throughout the spectrum in which the device may operate. Several inadequacies of this concept exist because the amount of energy necessary to reliably jam a small surveillance transmitter can be enormous. Consequently, this hash generation also interferes with local radio and television sets and the two-way communications of aircraft, police and emergency vehicles operating in the vicinity.

A simple jammer is shown in figure 30.

The only devices available for protection against carrier current devices on both telephone lines and power lines are absorptive line filters. These filters prevent the passage over wires of frequencies above the audio range and severely attenuate the normally used carrier current spectrum between 20 KHz and 500 KHz. Power line filters tend to be bulky because of power handling requirements, and such a device for each power line may be 2 to 3 feet in length and 4 or more inches in diameter. Those suitable for use on telephone lines are significantly smaller. Carrier current power line filters are readily available and are frequently used in conjunction with r-f shielded rooms. In a security application these filters are placed on the lines exiting the security area and require proper installation and grounding. These filters cost \$500 to \$1000 each depending on power handling requirements of the secure area.

Active jamming of surveillance tape recorders has been rumoured in various publications, and this phenomenon does exist in limited situations. Theoretically, a 60 KHz signal is injected into a telephone or other suspect wire and, if these lines are connected to a susceptible tape recorder, this 60 KHz signal can upset the recording system and reduce the quality of the recorded conversation. Use of this technology for security purposes is more the exception than the rule since the susceptibility of recording systems to this kind of jamming varies widely. Signals of this frequency are occasionally used for tape erasing, but they do not travel far along a telephone line or maintain sufficient strength to have a

significant effect upon a properly connected tape recording system.

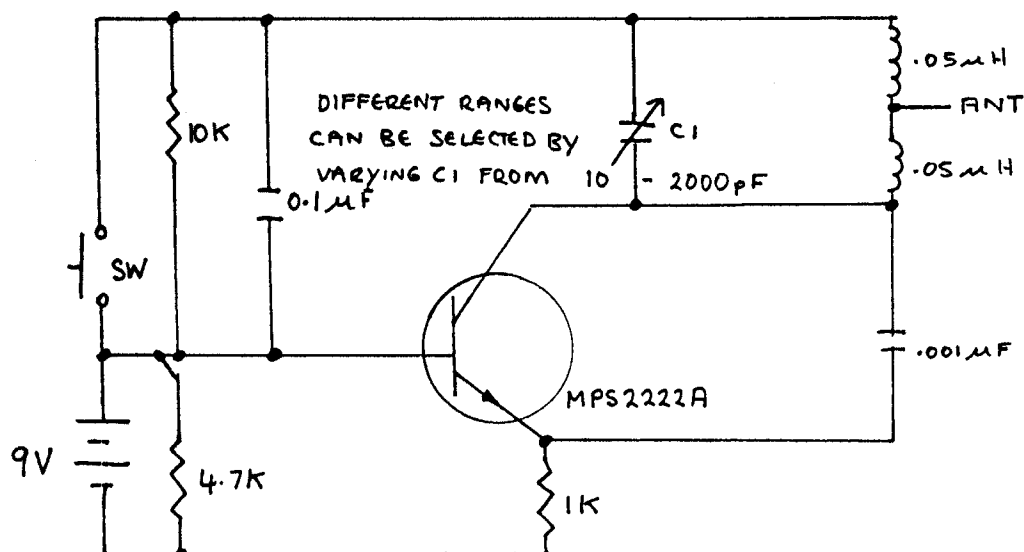


Figure 30: Radio Frequency Jammer.

GLOSSARY

BANDWIDTH The extent or deviation of frequencies about a given centre frequency. Also, characteristic of a radio receiver which allows information of a certain frequency and bandwidth to be received.

CARRIER Radio-frequency signal of constant amplitude upon which information may be added by means of modulation.

COHERENT Electromagnetic energy where all individual waves of one frequency are locked in phase in orderly fashion compared to non-coherent waves which are random.

DEMODULATION Process of retrieving audio information from a modulated r-f signal.

FILTER Electrical circuit that accepts (or rejects) a particular band of frequencies.

FREQUENCY MODULATION (FM) Method of modulation by which intelligence is impressed on a carrier by varying the frequency of the carrier.

HASH Electrical noise.

HOOK SWITCH Switch in telephone instrument actuated by the plunger on which the handset rests when not in use.

IMPEDANCE Resistance to the flow of alternating current. The combined effect of resistance, inductance and capacitance.

IMPEDANCE MATCHING The circuit arrangement required to adjust the impedance of an alternating current circuit to the value recommended for proper operation.

MODULATOR Electronic circuitry used to impress information on a carrier by instantaneously varying its amplitude (AM) or frequency (FM).

NARROW BAND FM Special form of FM modulation where the deviation caused by the modulation process about the main carrier is less than normal.

RESONANT CAVITY Hollow metal cylinder whose dimensions are chosen to make it strongly reflect a radio signal of predetermined frequency.

SIDE BAND The small band of frequencies produced adjacent to a main radio carrier frequency which contains the basic audio information.

VOICE ACTIVATED SWITCH (VOX) Switch that closes when conversation is impressed at its input. Used to turn electronic devices on and off.

